(19)世界知识产权
组织国
际局。

(注 43)国际出版日期 2020 年 3 月 26 日(26.03.2020)。

(10)国际出版编号。
WO 2020/060606。

pct。
ONE OR ET 翻译

(51)国际专利分类：
G06Q 20/06(2012.01)G06Q 30/02(2012.01)。
G06Q 20/32(2012.01)G06N3/08(2006.01)。
H04L 9/32(2006.01)。

(21) 国际申请编号：
%/美国 2019/038084。

(22) 国际申请日期：
2019 年 6 月 20 日(20.06.2019 年)。

(25) 备案语言：英语。

(26) 出版物语言：英语。

(30)优先级数据：
16/138,518 2018 年 9 月 21 日(21.09.2018)美国。

(71)申请人：微软技术许可有限责任公司[美国/美国]；**One Microsoft** Way，华盛顿州雷蒙德，98052-6399(美国)。

(72)发明人：**微软技术许可有限**责任公司，One Microsoft Way，华盛顿州雷蒙德，98052-6399(美国)。**微软技术许**可有限责任公司，One Microsoft Way，华盛顿州雷蒙德，98052-6399(美国)。**微软技术许可有限责任公**司，One Microsoft Way，华盛顿州雷蒙德，98052-6399(美国)。

(74)代理：**微软技术许可有**限责任公司，One Microsoft Way，华盛顿州雷蒙德市，98052-6399(美国)。

(81)指定国家(除*非另有说明，否则为所有可获得的国家保护*)：AE、AG、AL、AM、AO、AT、AU、Az、BA、BB、BG、BH、BN、BR、BW、B 乙 CA、CH、CL、CN、CO、CR、CU、CZ、DE、DJ、DK、DM、DO、D 乙 EC、EE、EG、ES、FI、GB、GD、GE、GH、GM、GT、HN、HR、HU、ID、IL、IN、IR、IS、JO、JP、KE、FI、GB、GD、GE、GH、GM、GT、HN、HR、HU、ID、IL、IN、IR、IS、JO、JP、KE。LY，MA，MD，ME，MG，MK，MN，MW，MX，“MZ，NA，NG，NI，NO，NZ，OM，PA，PE，PG，PH，PL，PT，QA，RO，RS，RU，RW，SA，

(54)**职称**：使用身体活动数据的加密货币系统。

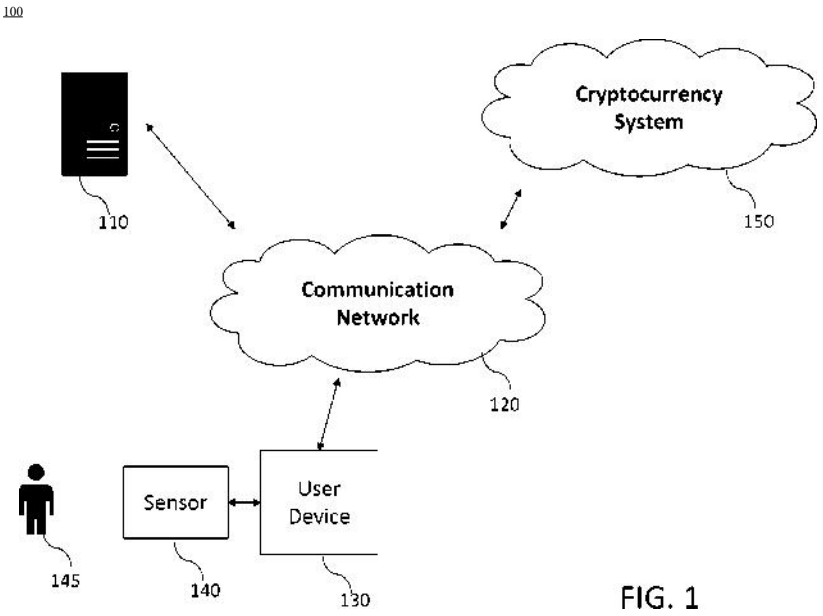


FIG. 1

(57)**摘要**：可以在加密货币系统的挖掘过程中使用与提供给用户的任务相关联的人体活动。服务器可以向通信地耦合到服务器的用户设备提供任务。通信地耦合到用户的设备或包括在用户的设备中的传感器可以感测用户的身体活动。可以基于感测到的用户的身体活动来生成身体活动数据。通信地耦合到用户的设备的加密货币系统可以验证主体活动数据是否满足由加密货币系统设置的一个或多个条件，并将加密货币奖励给其主体活动数据被验证的用户。

[下一页续]。

SC、SD、SE、SG、SK、SL、SM、ST、SY、TH、TJ、TM、TN、TR、TT、TZ、UA、UG、US、UZ、VC、VN、ZA、ZM、ZW。

(84)指定国家(除*非另有说明，否则包括所有可用的区域保护*)：Aripo(BW、GH、GM、KE、LR、LS、MW、MZ、NA、RW、SD、SL、ST、S 乙 TZ、UG、ZM、ZW)、欧亚(AM、Az、BY、KG、KZ、RU、TJ、TM)、欧洲(AL、AT、BE、BG、CH、CY、CZ、DE、DK、EE、ES、FI、FR、GB、GR、HR、HU、IE、IS。TR)、OAPI(BF、BJ、CF、CG、CI、CM、GA、GN、GQ、GW、KM、ML、MR、NE、SN、TD、TG)。

规则 4.17 下的声明：

— *关于申请人申请 FAR 和获批予专利的权利(规则 4.17(H))。*

— *关于申请人要求较早申请的优先权的权利(规则第 4.17(Iii)条)。*

发表：

— *与国际检索报告(第 21 条第(3)款)。*

使用身体活动数据的加密货币系统。

背景

[0001]虚拟货币(也称为数字货币)是一种交换媒介，通常通过互联网实现，不与特定的政府支持的“平面”(印刷)货币(如美元或欧元)捆绑在一起，通常旨在实现即时交易和无国界的所有权转移。虚拟货币的一个例子是加密货币，其中加密技术被用来保护交易和控制新单位的创建。

[0002]存在多种加密货币。其中，最广为人知的是基于区块链的加密货币。大多数基于区块链的加密货币都是分散的，因为它没有中央控制点。然而，基于区块链的加密货币也可以在具有对加密货币的中央控制点的集中式系统中实现。比特币是基于区块链的加密货币的例子之一。中本聪(Satoshi Nakamoto)在 2008 年的一篇文章中描述了这一点，这篇文章的标题是“比特币：一个点对点的电子现金系统“。

[0003]区块链是存储交易列表的数据结构，可以被认为是记录源标识符和目的地标识符之间的交易的分布式电子分类账。事务被捆绑到块中，并且每个块(第一个块除外)都指向或链接到区块链中的前一个块。计算机资源(或节点等)。维护区块链并以密码方式验证每个新块和包含在相应块中的事务。这个验证过程包括从计算上解决一个难题，这个难题也很容易验证，有时被称为工作证明。这个过程被称为“挖掘”。挖掘可能是一个概率很低的随机过程，因此要解决一个计算困难的问题需要进行大量的试错。因此，采矿可能需要大量的计算能量。

[0004]关于这些和其他一般考虑，已经描述了以下实施例。此外，尽管已经讨论了相对具体的问题，但是应该理解，实施例不应局限于解决背景中识别的特定问题。

摘要。

[0005]本公开的一些示例性实施例可以使用与提供给用户的任务相关联的人体活动作为在。

加密货币系统。例如，当用户执行信息或服务提供商提供的任务(例如查看广告或使用某些互联网服务)时，用户发出的脑波或体温可以用于挖掘过程。基于用户的身体活动产生的数据可以是工作证明，而不是一些传统的加密货币系统需要的大量计算工作，因此，用户可以在不知不觉中解决计算困难的问题。因此，本公开的某些示例性实施例可以降低挖掘过程的计算能量，并使挖掘过程更快。

[0006]这里为使用人体活动数据的加密货币系统提供了计算机可读存储介质的系统、方法和硬件方面。根据本公开的各种实施例，服务器可以向通信地耦合到服务器的用户的设备提供任务。可通信地耦合到或包括在用户设备中的传感器可以感测用户的身体活动，可以基于感测到的用户的身体活动来生成身体活动数据。通信地耦合到用户的设备的加密货币系统可以验证身体活动数据是否满足由加密货币系统设置的一个或多个条件，并将加密货币奖励给其身体活动数据被验证的用户。

[0007]示例被实现为计算机进程、计算系统或诸如设备、计算机程序产品或计算机可读介质的制品。根据一个方面，计算机程序产品是计算机系统可读的计算机存储介质，并且对包括用于执行计算机进程的指令的计算机程序进行编码。

[0008]提供该概要是为了以简化形式介绍一组概念，这些概念将在下面的详细描述中进一步描述。本摘要不旨在识别所要求保护的主题的关键特征或本质特征，也不旨在用于限制所要求保护的主题的范围。

附图的简要说明。

[0009]将参照附图描述根据本公开的各种实施例，其中：

[0010]图 1.。1 示出了其中可以实施本公开的一些示例性实施例的示例性环境；

[0011]图 1.。2 显示了一个分散的加密货币系统的系统图，根据。

涉及本公开的示例性实施例；

[0012]图 3.。3 示出了根据本公开的示例性实施例的计算机实现的方法的流程图；

[0013]图 3.。4 示出根据本公开的示例性实施例的用于生成身体活动数据的操作的流程图；

[0014]图 1.。5 示出根据本公开的示例性实施例的用于验证身体活动数据的操作的流程图；

[0015]图 3.。6 示出根据本公开的示例性实施例的区块链和区块链的两个示例性块；

[0016]图 1.。图 7 示出了根据本公开的另一个示例性实施例的使用向量重新嵌入的计算机实现的方法的流程图。8 示出了其中可以实现在此描述的系统、方法和计算机程序产品中涉及的处理的计算机或处理系统的示例性框图。

[0018]除非另有说明，否则不同附图中相应的数字和符号通常指的是相应的部件。这些图是为了清楚地说明实施例的相关方面而绘制的，并且不一定是按比例绘制的。

实施例的详细描述。

[0019]在下面的详细描述中，参考形成其一部分的附图，并且附图中通过图解的方式示出了可以实施本发明的具体实施例。对这些实施例进行了足够详细的描述，以使本领域技术人员能够实践本发明，并且应当理解，可以利用其他实施例，并且可以在不背离本发明的精神和范围的情况下进行结构、逻辑和电气上的改变。因此，下面的详细描述不是在限制意义上进行的，并且本发明的范围仅由所附权利要求及其等价物限定。附图中的类枚举指的是类似的部件，这从使用上下文中应该是显而易见的。

[0020]术语“加密频率”可以指一种数字货币，其中使用加密技术来管理货币单位的生成并验证其转账。许多加密货币包括使用区块链来提供安全和防止欺诈，因为这是双重支出。本公开的一些实施例可以在区块链之外的替代加密货币机制中使用。这里描述的系统、方法和计算机程序产品可以应用于集中式和。

分散的加密货币网络或数据库。

[0021]图 2.。1 示出了其中可以实践本公开的一些示例性实施例的示例性环境 100。示例环境 100 包括但不限于任务服务器 110、通信网络 120、用户设备 130、传感器 140 和密码货币系统 150 中的至少一个。

[0022]任务服务器 110 可以通过通信网络 120 向用户设备 130 提供一个或多个任务。例如，任务服务器 110 可以是递送或提供网页的 web 服务器、处理用户与应用程序或数据库之间的应用程序操作的应用程序服务器、云服务器、数据库服务器、文件服务器、服务服务器、实现游戏或游戏服务的游戏服务器、以及递送诸如流式视频或音频的媒体的媒体服务器中的至少一个。下面将更详细地讨论由任务服务器 110 提供的任务。

[0023]或者，加密货币系统 150 可以向用户设备 130 提供一个或多个任务。例如，在分散的加密货币网络中，任务可以由挖掘器(例如，图中的计算资源或节点 210)向用户设备 130 提出。2)。在另一示例中，在集中式加密货币系统中，加密货币服务器可以向用户设备 130 发送任务。

[0024]通信网络 120 可以包括任何有线或无线连接、互联网或任何其他形式的通信。尽管在图 1 中标识了一个网络 120。1 中，通信网络 120 可以包括图 1 中所示的任何服务器、设备、资源和系统之间的任意数量的不同通信网络。1 和 2 和/或这里描述的其他服务器、设备、资源和系统。通信网络 120 可以实现各种计算资源或设备、服务器和系统之间的通信。通信网络 120 的各种实现可以采用不同类型的网络，例如但不限于计算机网络、电信网络(例如，蜂窝)、移动无线数据网络、以及这些和/或其他网络的任意组合。

[0025]用户设备 130 可以包括能够处理和存储数据/信息并通过通信网络 120 进行通信的任何设备。例如，用户设备 130 可以包括个人计算机、服务器、蜂窝电话、平板电脑、膝上型计算机、智能设备(例如，智能手表或智能电视)。图中示出了用户设备 130 的示例性实施例。6.。

[0026]传感器 140 可以被配置成感测用户 145 的身体活动。如图所示。1，传感器 140 可以是与用户设备 130 分开的组件。

和/或通信地连接到用户设备 130。或者，传感器 140 可以包括并集成在用户设备 130 中。例如，用户设备 130 可以是其中具有传感器 140 的可穿戴设备。传感器 140 可以向用户设备 130 发送信息/数据。传感器 140 可以包括例如但不限于功能性磁共振成像(FMRI)扫描仪或传感器、脑电图(EEG)传感器、近红外光谱(NIRS)传感器、心率监视器、热传感器、光学传感器、射频(RF)传感器、超声波传感器、照相机或可以测量或感测身体活动或扫描人体的任何其他传感器或扫描仪。例如，功能磁共振成像可以通过检测与血流相关的变化来测量身体活动。功能磁共振成像可以使用磁场和无线电波来创建身体的详细图像(例如，大脑中的血液流动来检测活动区域)。 材料。()Http://news.berkely.edu/2011/09/22/BRain-movies/。展示了 fMRI 如何测量与视觉信息相关的大脑活动并生成图像数据的一个例子。

[0027]加密货币系统 150 可以包括用于处理命令的一个或多个处理器，以及以一个或多个加密货币数据结构存储信息的一个或多个存储器。在一些实施例中，加密货币系统 150 可以是集中式加密货币系统或网络，例如但不限于，可以由第三方实体或运行任务服务器 110 的同一实体私下运行的服务器。在其他实施例中，加密货币系统 150 可以是公共可访问的网络系统(例如，分布式分散计算系统)。

[0028]例如，如图所示，加密货币系统 150 可以是分散式网络 200，例如包括一个或多个计算资源 210 的分散式区块链网络。2.。在图 2 的实施例中。2，可能没有控制加密货币网络 200 的中央机构。存储在区块链网络 200 上的数据(即公共分类账)可能不会全部存储在中心位置。区块链网络 200 可以包括用于处理命令的多个处理器和以一个或多个区块链数据结构存储信息的多个存储器。区块链网络 200 可以维护连续增长的数据块列表的一个或多个区块链，其中每个数据块引用其列表上的先前块。要求每个区块引用区块链中的所有先前的区块，从而产生防止篡改和修改的区块链，从而区块链中存储的信息是不可变的。

[0029]计算资源 210 可以包括加入区块链网络 200 并在区块链网络 200 中形成节点的任何设备、计算机、系统或其他。算出。

资源 210 可以包括例如但不限于个人计算机、服务器、蜂窝电话
、平板电脑、膝上型计算机、智能设备(例如智能手表或智能电
视)或能够在通信网络 120 上存储信息和通信的任何其他设备。
在一些实施例中，计算资源 210 可以彼此独立或彼此未知，其
中例如计算资源 210 保持匿名。每个计算
机资源 210 可以包括存储器 220，其存储区块链网络 200 的公共账簿 230 的至少
一部分的副本。计算资源 210 还可以执行一个或
多个程序来执行与维护区块链网络 200 相关联的各种功能
，包括例如更新公共分类帐 230、生成新块或任何其他类似功
能。

[0030]为了说明起见，图 3.。1 示出未包括在区块链网络 200 中的用
户设备 130。然而，用户设备 130 可以是区块链网络 200 的一部分，
并且被实现为图中的计算资源 210 之一。2.。

[0031]公共分类帐 230 可以存储在区块链网络 200 上执行的任何交易，包括但不
限于例如与区块链网络 200 相关并在区块链网络 200 上发生的任何交易。
因为每个计算资源 210 存储区块链网络 200 的公
共分类账 230 的至少部分的副本，所以公共分类账 230 可以在任何
时间通过比较存储的多计算机资源 210 的副本来独立地验证准确性。

[0032]计算资源 210 之间通信可以通过通信网络 120 进行。
图 2 的通信网络 120。2 可以是与图 2 的通信 120 相同的
网络，也可以是与图 2 的通信 120 不同的网络。1.。在一些实施例中，每个
计算机资源 210 可以直接与其他计算资源 210 通信。在
一些实施例中，一些计算资源 210 可能不能彼此直接
通信。在这种情况下，计算机资源 210 之间与
区块链网络 200 相关的通信可以通过使用一
个或多个剩余计算资源 210 作为媒介来发生。
在一些实施例中，一个或多个计算资源 210 可
能不会一直保持到区块链网络 200 的连续连接。例如，
计算机资源 210 可以仅在每天的特定时间段期间连接到区
块链网络 200，或者可以仅间歇性地全天连接到区块链网络 200。
由于区块链网络 200 的分散性质，由一个或多
个计算资源 210 进行的这种间歇连接不影响区块链网络 200 的整
体操作，因为公共分类帐 230 的副本存储在多个。

计算资源 210。一旦断开的计算资源 210 重新连接到区块链网络 200，断开的计算资源 210 就可以从已经连接到区块链网络 200 的一个或多个计算资源 210 接收公共分类账 210 的更新副本。

[0033]图 3.。3 示出了根据本公开的示例性实施例的计算机实现的方法的流程图。

[0034]方法 300 开始于图 310 所示的操作 310。所述任务包括但不限于，在一定时间内观看或收听信息(例如，广告)、使用服务(例如，搜索引擎、聊天机器人、电子邮件、社交媒体/网络服务和任何因特网或 web 服务)、向网站、服务器或网络(例如，内容共享网站和云网络或服务器)上传或发送信息/数据，或者可以产生效果的任何其他信息或服务，其中任务服务器 110 通过通信网络 120 向用户 145 的设备 130 提供一个或多个任务，所述任务包括但不限于，在一定时间内观看或收听信息(例如，广告)、使用服务(例如，搜索引擎、聊天机器人、电子邮件、社交媒体/网络服务和任何因特网或 web 服务)、或者向网站、服务器或网络(例如，内容共享网站、云网络或服务器)上传或发送信息/数据。任务可以作为交易包括在公共分类账 230 中。

[0035]此外，由任务服务器 110 提供的一个或多个任务可以包括解决用于区分人和机器输入以便人而不是计算机能够被动的测试，诸如区分计算机和人的计算机自动化程序(CAPTCHA)和旨在确立计算机用户是人类的类似 CAPTCHA 的系统 ReCAPTCHA。

该任务可以要求用户 145 解决验证挑战，例如，但不限于，基于图像的挑战，该挑战包括提示用户 145 通过与一个或多个图像交互来解决挑战的指令。

[0036]在操作 320，当用户 145 执行由任务服务器 110 提供的任务时或之后，传感器 140 可以感测用户 145 的身体活动，该身体活动是与任务服务器 110 提供的任务相关的身体响应，然后将感测到的用户 145 的身体活动发送到用户设备 130。

身体活动可以包括例如但不限于从人体发射的辐射、脑活动、体液流动(例如血液流动)、器官活动或运动、身体运动以及可以由图像、波、信号、文本、数字、度或任何其他形式的信息或数据感知和表示的任何其他活动。从人体发射的身体辐射的示例可以包括身体的辐射热、脉率或脑波。脑波可以包括，例如，但不限于，(I)参与学习或记忆任务的伽马波，(Ii)参与逻辑思维和/或有意识思维的 β 波，(Iii)可能与潜意识思维有关的阿尔法波，(Iv)可能与深沉和粗暴情绪有关的 θ 波，(V)可能涉及睡眠或深度放松的三角波，或(Vi)。

脑电图(EEG)，可以用来评估大脑的电活动，
如深度集中。身体运动的例子可能
包括眼睛运动、面部运动或任何其他肌肉运动。此外，使用
功能磁共振成像可以感觉到大脑活动。功能磁共振成像通过检测与血流相
关的变化来测量大脑活动。这项技术依赖于大脑血流和神
经元激活相耦合的事实。当大脑的某个区域在使用时，流向
该区域的血液也会增加。

[0037]在操作 330，用户设备 130 基于传感器 140 感测到的身体活动生成身体活动数据
。操作 330 可以是挖掘过程的一部分，该挖
掘过程是用于解决计算困难问题的过程。图 3 中示出了操作 330 的
一个示例性实施例。4.。如图所示。4，操作 330 可以包括操作 410
和 420。

[0038]在操作 410，传感器 140 感测到的身体活动可以被编码为符号
形式，例如字母、数字、符号和包括字符序列的字符串。
在一个示例中，可以通过从感测到的身体活动中提取
一个或多个值(例如身体活动信号(例如，脑波)的最小和/
或最大幅度或频率)来对身体活动进行编码。在另一示例中，用户设
备 130 可以对感测到的身体活动随时间开窗并采样，并计算采样
值的平均值。在又一示例中，用户设备 130 可以生成身体活动的
原始数据。在又一示例中，在操作 420，用户设备 130 可以使用一个或
多个滤波器来过滤身体活动的原始信号，以将过滤后的身体活动信号应
用于音频散列函数或算法。或者，与人体活动相关联的任何
统计值都可以从传感器 140 感测到的身体活动编码。

[0039]在操作 420，可以通过使用诸如散列算法或函数的加密算法将
编码的主体活动转换成加密的输出。例如，
散列函数包括映射输出数据集的初始输入数据集的函数。通常
，散列函数可以是可用于将任意大小的数据映射到固定大小
的数据的任何函数。散列函数允许人们轻松地验证某些输入数据映
射到给定的散列值，但是如果输入数据是未知的，则故意难以
通过知道存储的散列值来重建它(或任何等效的替代方案)。该算
法或函数可以包括在加密货币系统或数据库
的挖掘软件或程序中。

[0040]例如，操作 420 可以使用音频散列函数，其中将编码的身体活动
的频率的直方图相加，或者使用比特操作，诸如异或。

对编码的身体活动执行具有下一个或素数模数
的每个直方图桶的函数。

[0041]在一些实施例中，可以使用身体活动本身是散列的模拟散列函数。例如，由传感器 140 感测到的波或信号，例如但不限于来自 EEG 传感器的 α 、 β 、 δ 或伽马波，可以使用变换算法或公式(例如快速傅立叶变换(FFT)或可以卷积、相加或相乘以产生直方图的任何其他算法或公式)变换为直方图。散列可以是直方图本身。例如，散列可以是 FFT 的输出，其中每个分量是频带，并且值是对应于每个频带的计数。在另一示例中，例如，所需的属性可以是前两个频率直方图尽可能接近于零，前提是存在某种统计保证，即这不容易发生。

[0042]然而，操作 420 是可选的。在某些实施例中，用户设备 130 可以将在操作 410 生成的编码身体活动发送到加密货币系统 150，而不加密或散列编码的身体活动。

[0043]尽管图 4 所示的。3 示出包括操作 410 和 420 的操作 330 由用户设备 130 处理，操作 410 和 420 中的至少一个可以由诸如任务服务器 110、密码货币系统 150 或任何其他服务器的另一个或多个设备、服务器、资源或系统处理。例如，用户设备 130 可以生成感测到的身体活动的原始数据，将其发送到密码货币系统 150、任务服务器 110 或任何其他服务器，然后密码货币系统 150、任务服务器 110 或任何其他服务器可以对感测到的身体活动的原始数据进行编码或散列。

[0044]回过头来参照图 2。3，在操作 340，加密货币系统 150 验证由用户设备 130 生成的用户 145 的身体活动数据是否满足由加密货币系统 150 的算法设置的一个或多个条件。这些条件可以通过模拟人体活动来设置，所有人体活动都可以构成散列。机器学习算法可用于模拟身体活动并设置有效身体活动的条件，例如但不限于使用生成性对抗性网络。

[0045]在一些实施例中，加密货币系统 150 验证用户 145 的身体活动数据(例如，在操作 410 产生的身体活动的代码或在操作 420 产生的身体活动的散列)是否可以表示用户 145 的身体活动在目标范围内。可以使用用户 145 执行由任务服务器 110 提供的任务所需的认知努力量来确定目标范围。例如，为了验证用户 145、加密货币系统 150。

可以确定例如但不限于(I)用户 145 的身体活动的散列是否具有由密码货币系统 150 设置的特定特定模式、重复模式、数学属性或前导数字、字符或串的数量(例如前导零)，或者(Ii)用户 145 的身体活动的散列是否小于当前目标值。加密货币系统 150 设置的数字模式的示例可以是散列的第一个特定数字形成质数的模式，或者通过将散列的第一个特定数字应用于预设公式而计算出的数字形成素数的模式(例如，通过将预定数字或由加密货币系统 150 设置的数字加或减到散列的前四位而计算出的数字形成质数)。重复数字模式可以包括重复数字(例如，前导 0、散列中间的 1、散列的最后四位数字中的两个、以及散列中包括的任何重复数字)和重复数字序列(例如，前导重复数字对，例如“121212”，或三元组“123123”)。如果用户 145 的身体活动的散列具有期望的模式或在目标范围内，则认为工作证明或赌注证明已解决，并且该散列可以是新的块。目标范围或值可以定期改变，以保持预先选择的难度水平，尽管这不是必需的。例如，目标值可能与难度成反比。通过改变难度，可以保持大致恒定的块生成速率。

[0046]可以使用统计数据来设置有效身体活动的目标范围，从而不能验证正常身体活动、容易发生的活动或伪装身体活动。例如，有效身体活动的目标范围可以从人类矿工不能伪造他们自己的身体活动以满足目标范围来证明和验证工作证明的范围中选择。

[0047]此外，操作 340 处的验证可以包括过滤掉无效任务、格式错误的数据(语法错误)或从未授权用户发送的或由机器学习系统生成的数据。例如，加密货币系统 150 可以从用户设备 130 接收在应用散列算法之前生成的身体活动的数据，对该数据进行重新散列，然后将重新散列的数据与从用户设备 130 接收的散列进行比较，以检查身体活动数据是否是基于人类而不是随机计算机生成的数据生成的。FMRI 的图像的体素可以是在应用散列算法之前生成的身体活动数据的示例。

[0048]图 3 中示出了操作 340 的一个示例性实施例。5.。在操作 510，加密货币系统 150 可以检查从。

用户设备 130 在由加密货币系统 150 设置的目标范围内，或者包括由加密货币系统 150 设置的所需模式。如果主体活动的散列在目标范围内或者具有由加密货币系统 150 设置的期望模式，则加密货币系统 150 重新散列在应用散列算法之前生成的主体活动的数据，并将其与来自用户设备 130 的主体活动的散列一起发送(操作 520)，然后将重新散列的数据与从用户设备 130 接收的主体活动的散列进行比较(操作 530)。如果重新散列的数据与从用户设备 130 接收的主体活动的散列相同，则密码货币系统 150 前进到操作 350。然而，如果在操作 510 中确定主体活动数据的散列超出目标范围或者不包括由密码流通系统 150 设置的期望模式，或者如果在操作 530 中确定重新散列的数据与主体活动的散列不匹配，则可以继续操作 310 或 320。

[0049]在操作 350，当从用户设备 130 发送的身体活动数据满足由加密货币系统 150 设置的一个或多个条件时，加密货币系统 150 将加密货币授予用户 145。例如，加密货币系统 150 向用户 145 授予对应于由用户 145 完成的任务的加密货币量。另外，加密货币系统 150 可以将加密货币奖励给任务服务器 110 的所有者或操作员，作为对提供诸如搜索引擎、聊天机器人、应用或网站的服务、向用户免费提供对付费内容(例如，视频和音频流或电子书)的访问、或与用户共享信息或数据的奖励。

[0050]例如，在区块链加密货币系统中，在操作 340，图 2 的计算资源 210 中的至少一个。2 验证用户 145 的身体活动数据的散列是否有效。在操作 350，当在操作 340 验证用户 145 的身体活动数据的散列时，图 3 的计算资源 210。2 可以向区块链添加新块。新块可以包含分配给用户地址的加密货币单元的数量。具有附加添加的区块的新区块链在加密货币网络 150 周围广播。执行操作 340 和 350 的计算资源 210 还可以获得交易费和/或加密货币奖励。

[0051]图 3.。5 描绘了根据本公开的示例性实施例的区块链 500 和区块链 500 的两个示例性块 510、520。通常，“区块链”被理解为包括一系列块的数据结构，其中每个块包括对应于一个或多个事务的数据，这些数据与链接数据一起散列在一起，诸如紧接在前的块的散列。在本公开的实施例中，交易可以是由用户 145 执行的任务。链条可以。

然后用于创建分类帐，该分类帐通常是一个仅附加的数据库。一旦数据被输入到链的块中，该条目基本上是不可反驳的，因为对数据的任何篡改都将反映在链式散列计算中，因此很容易被检测到。区块链 500 可以表示可公开分发的交易分类账，例如图 230 的分类账。2，并且可以包括多个块。诸如块 510 和块 520 的每个块可以包括关于最近事务的数据。例如，由用户 145 执行的任务和授予用户 145 的加密货币单元的数量，和/或将一个块 520 链接到前一块 510 的链接数据的内容，以及确保区块链 500 的状态有效并且由记录保存系统的大多数认可/验证的工作证明数据，例如，主体活动的经验证的散列。

区块链 500 的块 520 的示例性实施例可以包括 CURrenHash、先前块 510 的先前散列、事务。前一个散列是来自前一个块的散列，这确保每个块都与前一个块固定地联系在一起。前一块 510 的散列可以包括在块 520 中，从而将块 520 链接到前一块 510。

[0053]在没有至少一个计算机资源 210 注意的情况下，不能修改交易信息，因此，可以信任区块链 500 来验证在区块链 500 上发生的交易。

[0054]在一些实施例中，向量或嵌入可以用于身体活动数据。7 示出了使用矢量(或嵌入)的计算机实现的方法的示例性实施例的流程图。如上面参照图 3 详细描述的。任务服务器 110 或加密货币系统/网络 150(例如中央加密货币服务器或计算资源(或节点)210)可以执行操作 310，其中通过通信网络 120 向用户设备 130 建议一个或多个任务，并且传感器 140 可以执行操作 320，其中传感器 140 感测或测量用户 145 的身体活动。

传感器 140(或用户设备 130)可以生成图像、波形、信号、数字、字符、字符串或可以表示身体活动的任何其他形式的身体活动的数据。

[0055]在操作 710，用户设备 130 从传感器 140(或用户设备 130)生成的身体活动的数据产生一个或多个向量(或嵌入)，诸如浮点数数组。存储在用户设备 130 或通过通信网络 120 以通信方式连接到用户设备 130 的任何设备、服务器、系统或网络中的算法可以将传感器 140(或用户设备 130)生成的身体活动的数据转换成一个或多个向量。例如，大脑图像。

由 fMRI 扫描仪生成的数据可以被馈送到计算机视觉机器
学习算法中，例如但不限于卷积神经网络，并且机器学
习算法可以从脑图像的一个或多个体素生成一个或多个向量
。在一些实施例中，可以在操作 710 处生成一个单个向量。在
其他实施例中，当用户 145 正在执行任务时，可以通过随时间采样
来产生一系列矢量。身体活动(例如，脑图像的体素)和
/或矢量(或嵌入)的数据可以生成工作证明，并被发送
到密码系统/网络 150。

[0056]此外，向量可以可选地包括与任务相关的一个或多个向量
，例如但不限于用户 145 使用的搜索项或用户 145 查看的广告的标
识符。

[0057]在操作 720，可以通过使用加密算法(例如散列算法或函数)
将在操作 710 生成的向量转换为加密输出，如以上参考图的操作
420 所解释的。4.。例如，可以使用诸如安全散列
算法(SHA)-1、SHA-256、SHA-384、SHA-512 和消息摘要(MD)-5 之类的散列算法将向量散列为字节。

[0058]然而，操作 720 是可选的。在一些实施例中，用户设备
130 可以将在操作 710 产生的身体活动的向量发送到密码系统 150，而不
对其进行加密或散列。

[0059]在操作 730，密码货币系统 150 从用户设备 130 接收用户 145 的身体活动的
数据(例如，脑图像的体素)和/或用户 145 的身体活动的向量(或散列)。

[0060]在操作 740，加密货币系统 150 检查从用户设备 130 接收的向量是否具有由
加密货币系统/网络 150 设置的一个或多个数学属性。
例如，加密货币系统 150 可以确定身体活动的
一个或多个向量是否与由加密货币系统 150 的算法设置的合法向量(
或绝对线向量)具有相似性(或关系)。可以使用例
如但不限于余弦相似性、欧几里德距离、曼哈顿
距离、明可夫斯基距离和贾卡德相似性来测量或
计算相似性。可以基于执行相同任务的人的身体活动
向量具有一定程度的相似性的假设来设置合
法向量。加密货币系统 150，例如图中中央加密货币服务器/网络或计算资
源(或节点)210。例如，挖掘器喜欢图 210 的
计算资源(或节点)210。2 可以分享他们的证据。

例如，包括但不限于，身体活动的矢量与加密货币网络 150，并通过计算工作证明的平均值(例如，矢量的质心或加权平均值和标准偏差)来确定合法矢量和相似性。

[0061]如果从用户设备 130 接收的向量具有由加密货币系统/网络 150 设置的数学属性，则加密货币系统/网络 150 对从用户设备 130 发送的身体活动的数据进行重新散列(操作 750)，然后将重新散列的输出与从用户设备 130 接收的向量(或散列)进行比较(操作 760)。

例如图 2 的计算机资源(或节点)210。2 可以将从用户设备 130 发送的 fMRI 体素重新散列为矢量，然后将重新散列的矢量与从用户设备 130 接收的矢量进行比较，以检查身体活动数据是否是基于人类而不是随机计算机生成的数据生成的。如果在操作 740 中确定接收到的向量用户设备 130 不满足由加密货币系统/网络 150 设置的数学属性，或者如果在操作 760 中确定重新散列的输出与从用户设备 130 接收到的向量(或散列)不匹配，则可以继续操作 310 或 320。

[0062]如果重新散列的输出与从用户设备 130 接收到的向量(或散列)相同，则加密货币系统/网络 150 将加密货币授予用户 145，如上面关于操作 350 详细描述的。例如，在区块链加密货币系统中，诸如图 2 的计算资源(或节点)210 之一的挖掘器。执行主体活动数据验证的 2 可以向区块链添加包括主体活动的数据、向量(或散列)和/或分配给用户地址的加密货币单元的数量的新块，在加密货币网络 150 周围广播具有新块的新区块链，并且可以获得交易费和/或加密货币奖励。

[0063]图 3.。8 示出了在本公开的一个实施例中可以实现任何系统、方法和计算机程序产品的示例计算机或处理系统的示意图，所述系统、方法和计算机程序产品诸如任务服务器 110、用户设备 130、密码货币系统 150 和计算资源 210。该计算机系统仅是合适的处理系统的一个示例，并且不打算建议对在此描述的方法的实施例的使用范围或功能的任何限制。所示的处理系统可以与许多其他通用或专用计算系统环境或配置一起操作。可能适合使用的公知计算系统、环境和/或配置的示例。

利用图 1 中所示的处理系统。8 可以包括但不限于个人计算机系统、服务器计算机系统、瘦客户端、胖客户端、手持或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络 PC、小型机系统、大型计算机系统以及包括上述系统或设备中的任何一个的分布式云计算环境等。

[0064]通常，程序模块可以包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、逻辑、数据结构等。

该计算机系统可以在分布式云计算环境中实施，在分布式云计算环境中，任务由通过通信网络链接的远程处理设备执行。在分布式云计算环境中，程序模块可以位于本地和远程计算机系统存储介质中，包括存储器存储设备。

[0065]计算机系统 800 的组件可以包括但不限于一个或多个处理器或处理单元 810、系统存储器 820 以及将包括系统存储器 820 的各种系统组件耦合到处理器 810 的总线 830。处理器 810 可以包括执行这里描述的方法的软件模块 815。模块 815 可以被编程到处理器 810 的集成电路中，或者从存储器 820、存储设备 840、或网络 850 或其组合加载。

[0066]总线 830 可以表示几种类型的总线结构中的任何一种或多种，包括存储器总线或存储器控制器、外围总线、加速图形运动、以及使用各种总线体系结构中的任何一种的处理器或局部总线。作为示例而非限制，这样的体系结构包括工业标准体系结构(ISA)总线、微通道体系结构(MCA)总线、增强型 ISA(EISA)总线、视频电子标准协会(VESA)局部总线和外围部件互连(PCI)总线。

[0067]计算机系统 800 可以包括各种计算机系统可读介质，这些介质可以是计算机系统可访问的任何可用介质，并且可以包括易失性和非易失性介质、可移动和不可移动介质。

[0068]系统存储器 820 可以包括易失性存储器形式的计算机系统可读介质，诸如随机存取存储器(RaM)和/或高速缓冲存储器或其他。

易失性计算机系统存储介质。仅作为示例，可以提供存储设备 840 以用于从不可移动、非易失性磁介质(例如，硬盘驱动器)读取和写入到不可移动、非易失性磁介质。尽管未示出，但可以提供用于读写可移动、非易失性磁盘(例如，软盘)的磁盘驱动器，以及用于读写诸如 ACD-ROM、DVD-ROM 或其他光学介质的可移动、非易失性光盘的光学盘驱动器。在这种情况下，每个都可以通过一个或多个数据介质接口连接到总线 630。

[0069]计算机系统 800 还可以与诸如键盘、定点设备、显示器 870 等一个或多个外部设备 860、使用户能够与计算机系统交互的一个或多个设备、和/或使计算机系统能够与一个或多个其他计算设备通信的任何设备(例如，网卡、调制解调器等)通信，这样的通信可以通过输入/输出(I/O)接口 880 发生。

[0070]此外，计算机系统 800 可以经由网络适配器 855 与一个或多个网络 850 通信，例如局域网(LAN)、通用广域网(WAN)和/或公共网络(例如，因特网)。如图所示，网络适配器 855 通过总线 830 与计算机系统的其他组件通信。应当理解，尽管未示出，但是可以结合计算机系统使用其他硬件和/或软件组件。示例包括但不限于：微码、设备驱动器、冗余处理单元、外部磁盘驱动器阵列、RaID 系统、磁带驱动器和数据存档存储系统等。

[0071]如本领域技术人员将理解的，本公开的各方面可以实现为系统、方法或计算机程序产品。因此，本公开的各方面可以采取完全硬件实施例、完全软件实施例(包括固件、驻留软件、微代码等)的形式。或者结合软件和硬件方面的实施例，其在本文中可以统称为“电路”、“模块”或“系统”。此外，本公开的各方面可以采用包含在其上包含计算机可读程序代码的一个或多个计算机可读介质中的计算机程序产品的形式。

[0072]可以利用一个或多个计算机可读介质的任意组合。计算机可读介质可以是计算机可读信号介质或计算机可读存储介质。计算机可读存储介质可以是例如但不限于电子、磁、光、电磁、红外或半导体系统、装置或设备，或上述的任何适当组合。计算机可读存储介质的更具体的示例(非穷举列表)将包括。

便携式计算机磁盘、硬盘、随机存取存储器(RaM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM 或闪存)、便携式光盘只读存储器(CD-ROM)、光存储设备、磁存储设备或上述设备的任何适当组合。在本文档的上下文中，计算机可读存储介质可以是任何有形介质，其可以包含或存储由指令执行系统、装置或设备使用或结合指令执行系统、装置或设备使用的程序。

[0073]计算机可读信号介质可以包括其中包含计算机可读程序代码的传播数据信号，例如，在基带中或作为载波的一部分。这样的传播信号可以采取各种形式中的任何一种，包括但不限于电磁、光学或其任何适当的组合。计算机可读信号介质可以是任何计算机可读介质，该计算机可读介质不是计算机可读存储介质，并且可以通信、传播或传输供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合使用的程序。

[0074]包含在计算机可读介质上的程序代码可以使用任何适当的介质来传输，包括但不限于无线、有线、光缆、RF 等，或者前述的任何适当的组合。

[0075]用于执行本发明各方面的操作的计算机程序代码可以用一种或多种编程语言的任意组合来编写，所述一种或多种编程语言包括诸如 Java、Smalltalk、C++等的面向对象编程语言和诸如“C”编程语言或类似编程语言的常规过程编程语言、诸如 Perl、VBS 或类似语言的脚本语言、和/或诸如 Lisp 和 ML 的函数式语言以及诸如 Prolog 的面向逻辑的语言。

程序代码可以完全在用户的计算机上、部分在用户的计算机上、作为独立的软件包、部分在用户的计算机上和部分在远程计算机上或者完全在远程计算机或服务器上执行。在后一种情况下，远程计算机可以通过任何类型的网络连接到用户的计算机，包括局域网(LAN)或广域网(WAN)，或者可以连接到外部计算机(例如，使用因特网服务提供商通过因特网)。

[0076]参照根据本公开的一些实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图来描述本公开的各方面。应该理解的是，流程图的每个方框和/或方框图以及。

流程图和/或框图中的框可以由计算机程序指令来实现。这些计算机程序指令可以被提供给通用计算机、专用计算机或其他可编程数据处理设备的处理器以产生机器，使得经由计算机或其他可编程数据处理设备的处理器执行的指令创建用于实现流程图和/或框图块中指定的功能/动作的手段。

[0077]这些计算机程序指令也可以存储在计算机可读介质中，该计算机可读介质可以指导计算机、其他可编程数据处理设备或其他设备以特定方式运行，使得存储在计算机可读介质中的指令产生包括实现流程图和/或框图块中指定的功能/动作的指令的制品。

[0078]计算机程序指令还可以被加载到计算机、其他可编程数据处理设备或其他设备上，以使得在计算机、其他可编程设备或其他设备上执行一系列操作步骤以产生计算机实现的过程，使得在计算机或其他可编程设备上执行的指令提供用于实现流程图和/或框图块中指定的功能/动作的过程。

[0079]图中的流程图和框图说明了根据本发明的各种实施例的系统、方法和计算机程序产品的可能实现的体系结构、功能和操作。就此而言，流程图或框图中的每个框可以表示代码的模块、段或部分，其包括用于实现指定逻辑功能的一个或多个可执行指令。还应注意，在某些备选实现中，框中注明的功能可能以图中注明的顺序出现。例如，实际上，连续显示的两个块可以实质上同时执行，或者有时可以相反的顺序执行，这取决于所涉及的功能。还应注意的是，框图和/或流程图的每个框以及框图和/或流程图中的框的组合可以由执行指定功能或动作的基于专用硬件的系统、或专用硬件和计算机指令的组合来实现。

[0080]计算机程序产品可以包括能够实现这里描述的方法的所有相应特征，并且当加载到。

计算机系统--能够执行这些方法。在本上下文中，计算机程序、软件程序、程序或软件指的是一组指令的任何语言、代码或符号的任何表达，这些指令旨在使具有信息处理能力的系统直接或在以下任一项或两项之后执行特定功能：(A)转换为另一种语言、代码或符号；及/或(B)以不同的材料形式复制。

[0081]这里使用的术语仅用于描述特定实施例，并不意在限制本发明。这里使用的单数形式“a”、“an”和“the”意在也包括复数形式，除非上下文另有明确指示。还应当理解，当在本说明书中使用时，术语“包括”和/或“包括”指定了所陈述的特征、整数、步骤、操作、元素和/或组件的存在，但不排除存在或添加一个或多个其他特征、整数、步骤、操作、元素、组件和/或它们的组。

[0082]以下权利要求中的所有装置或阶跃功能元件(如果有的话)的相应结构、材料、动作和等价物旨在包括用于结合具体权利要求的其他权利要求元件执行该功能的任何结构、材料或动作。本发明的描述是为了说明和描述的目的而提出的，但并不打算以所公开的形式详尽地或局限于本发明。选择和描述实施例是为了最好地解释本发明的原理和实际应用，并使本领域的普通技术人员能够理解本发明的各种实施例，这些实施例具有适合于预期的特定用途的各种修改。

[0083]本公开的各个方面可以具体化为包含在计算机或机器可用或可读介质中的程序、软件或计算机指令，其使得计算机或机器在计算机、处理器和/或机器上执行时执行该方法的步骤。还提供了一种机器可读的程序存储设备，该程序存储设备有形地包含可由机器执行的指令程序，以实现本公开描述的各种功能和方法。

[0084]本公开的系统和方法可以在通用计算机或专用计算机系统上实现和运行。术语“计算机”

可以在本申请中使用的系统和“计算机网络”可以包括固定和/或便携式计算机硬件、软件、外围设备和存储设备的各种组合。计算机系统可以包括联网或以其他方式链接以协同执行的多个单独组件，或者可以包括一个或多个独立组件。本申请的计算机系统的硬件和软件组件可以包括并且可以包括在诸如台式机、膝上型计算机和/或服务器的固定和便携式设备内。模块可以是实现某些功能 77 的设备、软件、程序或系统的组件，其可以体现为软件、硬件、固件、电子电路等。

[0085]虽然已经描述了本发明的具体实施例，但是本领域的技术人员将理解，存在与所描述的实施例等效的其他实施例。因此，应当理解，本发明不限于具体说明的实施例，而仅限于所附权利要求的范围。

概念。

[0086]概念 1。一种加密货币系统，包括：一个或多个处理器；以及存储可执行指令的存储器，如果所述可执行指令由所述一个或多个处理器执行，则所述可执行指令将所述加密货币系统配置为：与用户的设备通信；接收基于所述用户的身体活动生成的身体活动数据，其中所述身体活动由通信耦合到所述用户的设备或包括在所述用户的设备中的传感器感测；验证所述用户的身体活动数据是否满足由所述加密货币系统设置的一个或多个条件；以及将加密货币奖励给其身体活动的用户。

[0087]概念 2。任何前面和/或后面的概念的系统，其中传感器感知的身体活动包括使用者发射的身体辐射、体液流动、脑波、脉率或身体热辐射中的至少一个。

[0088]概念 3。任何在前和/或在后概念的系统，其中基于与提供给用户的设备的任务相关联的人体活动量来设置一个或多个条件。

[0089]概念 4。任何在前和/或在后概念的系统，其中一个或多个条件包括身体活动数据表示用户执行提供给用户的设备的任务的条件。

[0090]概念 5。任何在前和/或在后的概念的系统，其中身体活动数据是使用散列算法生成的，该散列算法将人体活动转换为。

加密输出，并且所生成的身体活动数据包括用户的感测身体活动的散列。

[0091]概念 6。任何在前和/或在后概念的系统，其中身体活动数据包括由传感器检测到的身体活动产生的一个或多个向量。

[0092]概念 7。任何在前和/或在后概念的系统，其中所述一个或多个条件包括主体活动的散列包括重复模式或由加密货币系统设置的数学属性的条件。

[0093]概念 8。任何在前和/或在后概念的系统，其中所述加密货币系统通过为所授予的加密货币生成块并将所述块添加到存储在所述加密货币系统中的区块链来将所述加密货币授予所述用户。

[0094]概念 9。任何在前和/或在后概念的系统，其中该块包括数据，该数据包括：提供给用户的设备的任务；关于所授予的加密货币的信息；与主体活动相关联的散列；以及前一块的散列。

[0095]概念 10。任何在前和/或在后的概念的系统，其中提供给用户的设备的任务包括用于验证设备的用户是否是人类的测试。

[0096]概念 11。根据任何在前和/或在后概念的系统，其中，所述加密货币系统被配置为：从用户的设备接收在应用散列算法之前生成的主体活动的数据和主体活动的散列；对主体活动的数据进行重新散列；以及将重新散列的数据与从用户的设备接收的主体活动的散列进行比较，以验证主体活动数据。

[0097]概念 12。一种计算机实现的方法，包括：由耦合到网络的用户的设备通过网络接收任务；通过可通信地耦合到用户的设备或包括在用户的设备中的传感器感测用户的身体活动；基于感测到的用户的身体活动生成身体活动数据；通过通信耦合到用户的设备的加密货币系统验证身体活动数据是否满足由加密货币系统设置的一个或多个条件；以及由加密货币系统将加密货币授予。

[0098]概念 13。任何在前和/或在后的概念的方法，其中由传感器感测到的身体活动包括从以下位置发射的身体辐射中的至少一个。

使用者，体液流动，脑电波，脉搏频率或身体热辐射。

[0099]概念 14。如前面和/或后面的概念所述的方法，其中所述一个或多个条件由所述加密货币系统基于与提供给用户的设备的任务相关联的人体活动量来设置。

[00100]概念 15。如前面和/或后面的概念所述的方法，其中，验证身体活动数据是否满足一个或多个条件包括确定身体活动数据是否表示用户执行提供给用户的设备的任务。

[00101]概念 16。如前面和/或后面的概念所述的方法，其中，验证身体活动数据是否满足一个或多个条件包括确定身体活动数据是否表示由加密货币系统设置的多于一定数量的身体活动。

[00102]概念 17。如前面和/或后面的概念所述的方法，其中，使用将人体活动转换成加密输出的散列算法来生成身体活动数据，并且所生成的身体活动数据包括感测到的用户的身体活动的散列。

[00103]概念 18。任何在前和/或在后的概念的方法，其中身体活动数据包括从传感器感测到的身体活动产生的一个或多个向量。

[00104]概念 19。根据任何在前和/或在后概念的方法，其中验证身体活动数据是否满足由加密货币系统设置的一个或多个条件包括确定感测到的身体活动的散列是否包括由密码货币系统设置的重复模式或数学属性。

[00105]概念 20。如前面和/或后面的概念所述的方法，其中授予加密货币包括由加密货币系统生成用于授予的加密货币的块，并将生成的块添加到存储在加密货币系统中的区块链。

[00106]概念 21。根据任何在前和/或在后概念所述的方法，其中所述块包括数据，所述数据包括：提供给用户的设备的任务；关于所授予的加密货币的信息；所生成的与身体活动相关联的散列；以及先前块的散列。

[00107]概念 22。根据任何在前和/或在后概念的方法，其中该任务包括用于验证该设备的用户是否是人类的测试。

[00108]概念 23。任何在前和/或在后的概念的方法，

还包括：由加密货币系统从用户的设备接收在应用散列算法之前生成的身体活动的数据和主体活动的散列；由加密货币系统重新散列身体活动的数据；以及由加密货币系统将重新散列的数据与从用户的设备接收的身体活动的散列进行比较，以验证身体活动数据。

[00109]概念 24。一种设备，包括：通信地耦合到传感器的一个或多个处理器，传感器被配置为感测用户的身体活动；以及存储器存储可执行指令，如果由一个或多个处理器执行，则所述可执行指令将设备配置为：接收任务；基于感测到的用户的身体活动生成身体活动数据，其中感测到的身体活动与接收到的任务相关联；以及将所生成的身体活动数据发送到验证身体活动数据以奖励加密货币的系统或网络。

[00110]概念 25。任何在前和/或在后的概念的系统，其中由传感器感测到的身体活动包括从使用者发射的身体辐射、体液流动、脑波、脉率或身体热辐射中的至少一个。

[00111]概念 26。任何在前和/或在后概念的系统，其中使用将人体活动转换成加密输出的散列算法来生成身体活动数据。

[00112]概念 27。任何在前和/或在后概念的系统，其中身体活动数据包括从传感器感测到的身体活动产生的一个或多个向量。

[00113]概念 28。任何在前和/或在后概念的系统，其中，通过从传感器感测到的身体活动产生一个或多个向量并加密该一个或多个向量来生成身体活动数据。

索赔。

1. 一种加密货币系统，包括：

一个或多个处理器；以及。

存储可执行指令的存储器，如果所述可执行指令由所述一个或多个处理器执行，则将所述加密货币系统配置为：

与用户的设备通信；

接收基于用户的身体活动生成的身体活动数据，其中身体活动由通信地耦合到用户的设备或包括在用户的设备中的传感器感测；

验证用户的身体活动数据是否满足加密货币系统设置的一个或多个条件；以及。

将加密货币奖励给其身体活动数据经过验证的用户。

2. 如权利要求 1 所述的系统，其中由传感器感测到的身体活动包括从用户发射的身体辐射、体液流动、脑波、脉率或身体热辐射中的至少一个。

3. 如权利要求 1 所述的系统，其特征在于，所述一个或多个条件是基于与提供给用户的设备的任务相关联的人体活动量来设置的。

4. 根据权利要求 1-3 之一所述的系统，其中，所述身体活动数据是使用将人体活动转换为加密输出的散列算法生成的，并且所生成的身体活动数据包括感测到的所述用户的身体活动的散列。

5. 根据权利要求 1-3 之一的系统，其中，身体活动数据包括从传感器感测到的身体活动产生的一个或多个向量。

6. 根据权利要求 1-3 之一所述的系统，其中，所述加密货币系统通过为所奖励的加密货币生成块并将所述块添加到存储在所述加密货币系统中的区块链来将所述加密货币授予所述用户。

7. 如权利要求 6 所述的系统，其特征在于，所述块包括数据，所述数据包括：

提供给用户的设备的任务；

有关获奖加密货币的信息；

与身体活动相关联的散列；以及。

上一个块的哈希。

8. 如权利要求 3 所述的系统，其中，提供给用户的设备的任务包括用于验证设备的用户是否是人类的测试。

9. 如权利要求 4 所述的系统，其特征在于，所述加密货币系统被配置为：

从用户的设备接收在应用散列算法之前生成的身体活动的数据和身体活动的散列；

对身体活动的数据进行重新散列；以及。

将重新散列的数据与从用户的设备接收的身体活动的散列进行比较，以验证身体活动数据。

10. 一种计算机实现的方法，包括：

由耦合到网络的用户的设备通过网络接收任务；

由通信耦合到用户的设备或包括在用户的设备中的传感器感测用户的身体活动；

基于感测到的用户的身体活动来生成身体活动数据；

由通信耦合到用户的设备的加密货币系统验证主体活动数据是否满足由加密货币系统设置的一个或多个条件；以及。

由加密货币系统将加密货币授予其身体活动数据被验证的用户。

11. 根据权利要求 10 所述的方法，其中由传感器感测到的身体活动包括从用户发射的身体辐射、体液流动、脑波、脉率或身体热辐射中的至少一个。

12. 如权利要求 10 所述的方法，其特征在于，所述一个或多个条件由所述加密货币系统基于与提供给所述用户的设备的所述任务相关联的人体活动量来设置。

13. 根据权利要求 10-12 之一所述的方法，其中，使用将人体活动转换为加密输出的散列算法来生成身体活动数据，并且所生成的身体活动数据包括感测到的用户的身体活动的散列。

14. 根据权利要求 10-12 之一所述的方法，其中，所述身体活动数据包括从由所述传感器感测到的身体活动产生的一个或多个向量。

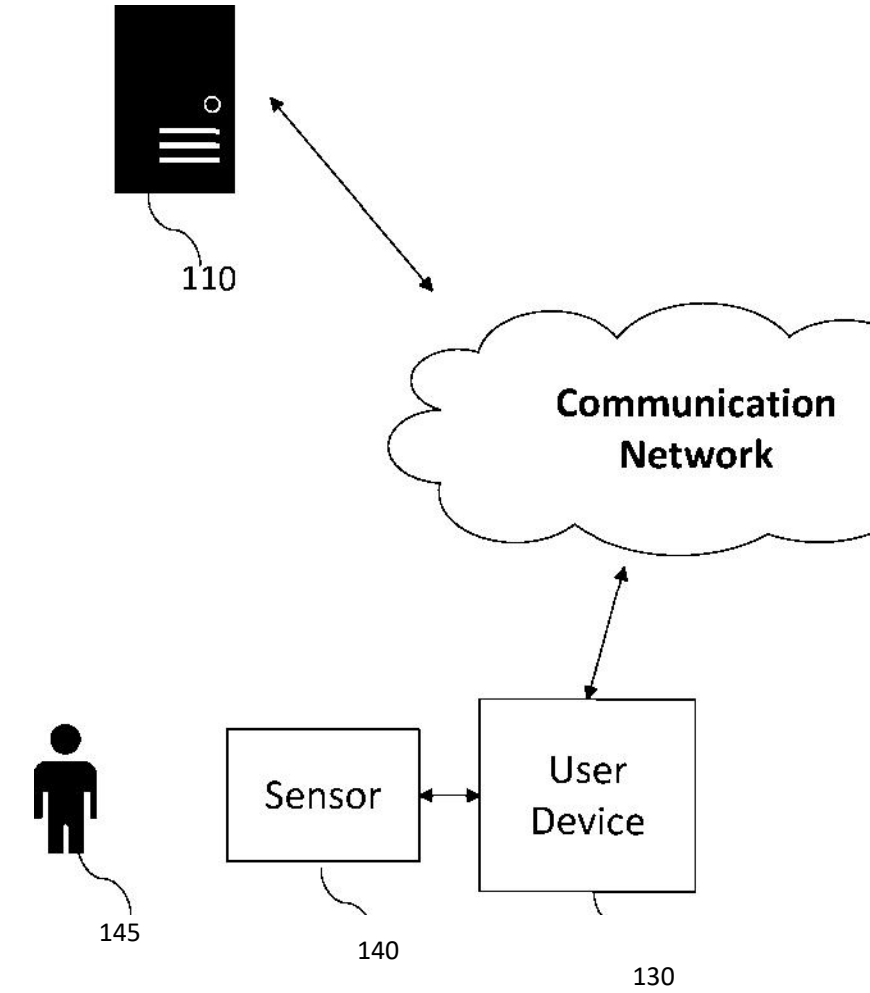
15. 根据权利要求 13 所述的方法，还包括：

加密货币系统从用户的设备接收在应用散列算法之前生成的主体活动的数据和主体活动的散列；

由所述加密货币系统对所述主体活动的数据进行重新散列；以及。

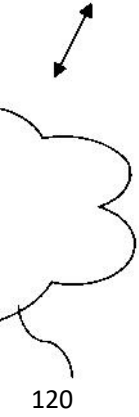
加密货币系统将重新散列的数据与从用户的设备接收的主体活动的散列进行比较，以验证主体活动数据。

100



我。

CryptocURrencySyste
m。



插图。1

200(150)。

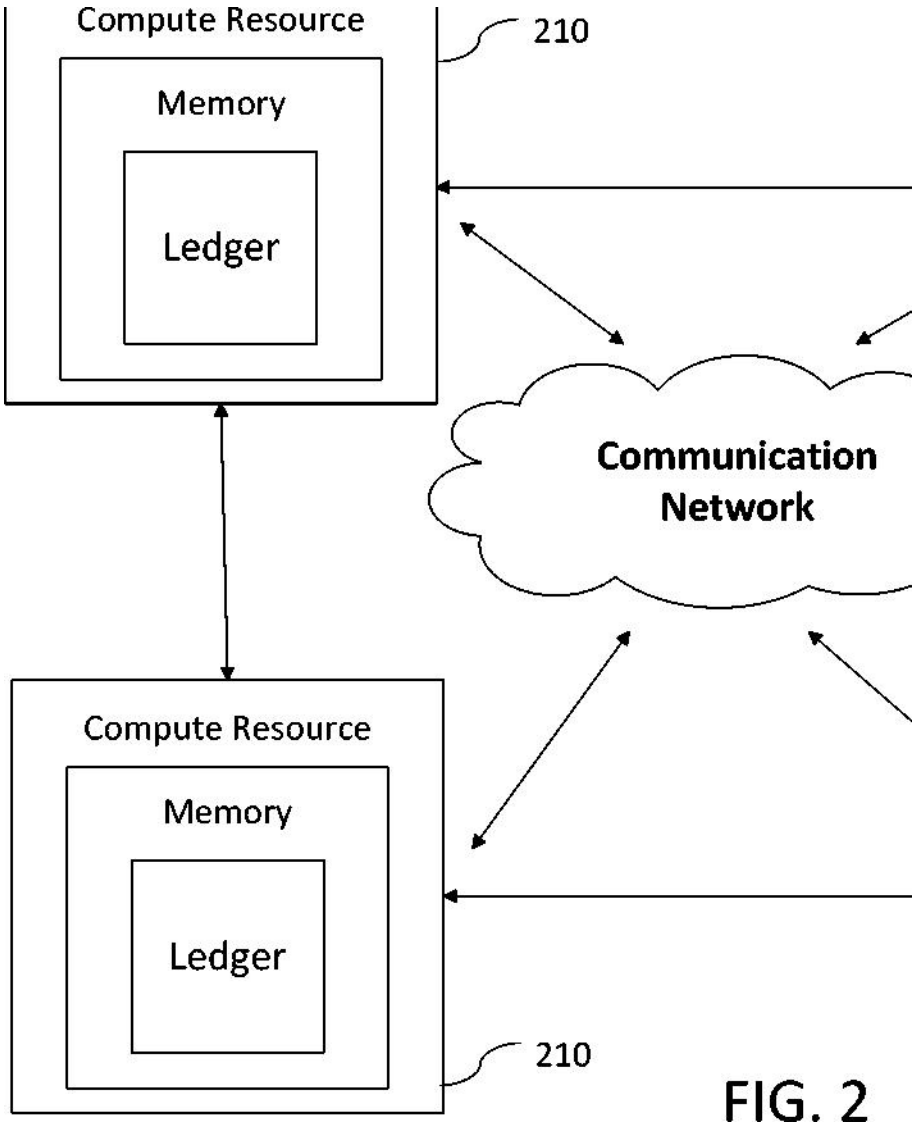
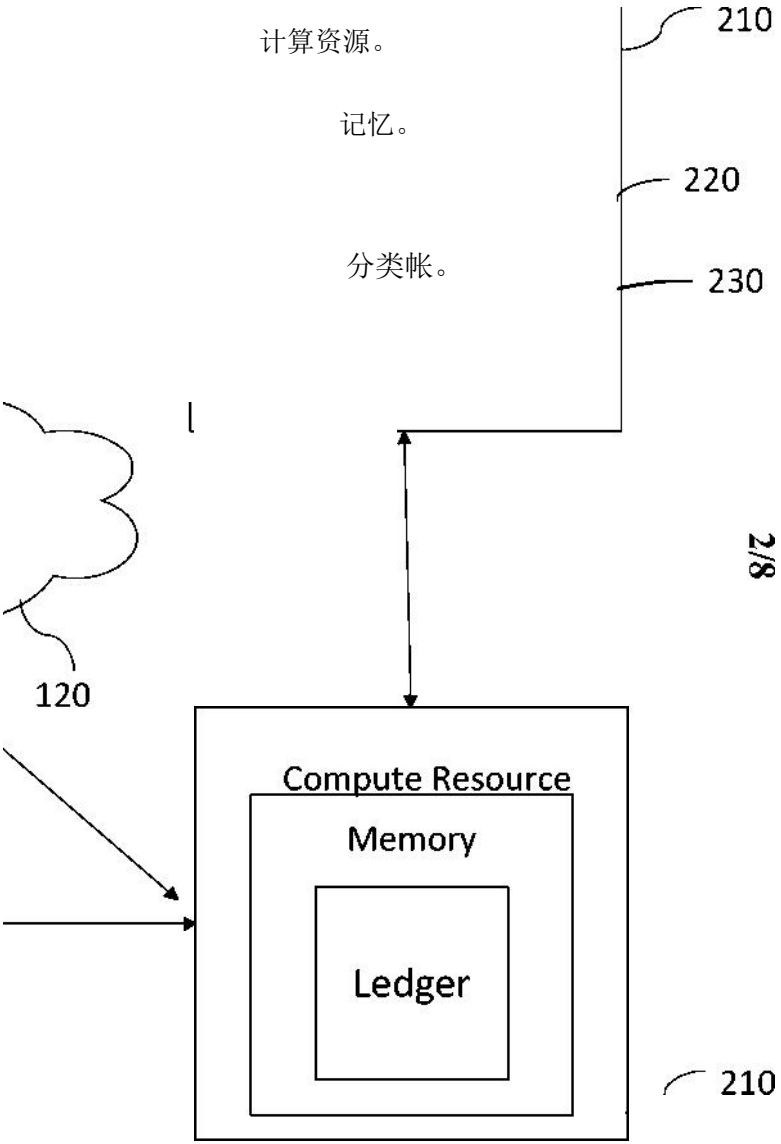

Compute Resource
Memory
Ledger
210
Communication Network
Compute Resource
Memory
Ledger
210

FIG. 2

计算资源。

记忆。

分类帐。



300

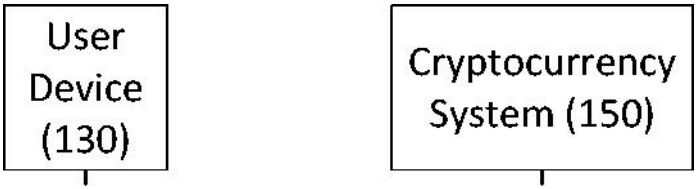
任务
服务器
(110)。

传感器。
(140)。

_____ I 310 I。
提供任务。 ----------
我。

检测用户二
正文活动。

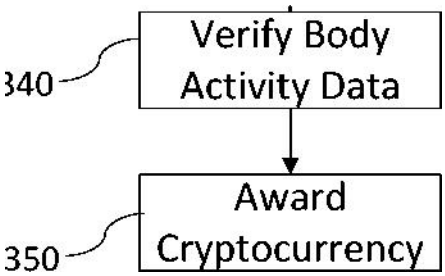
插图。3



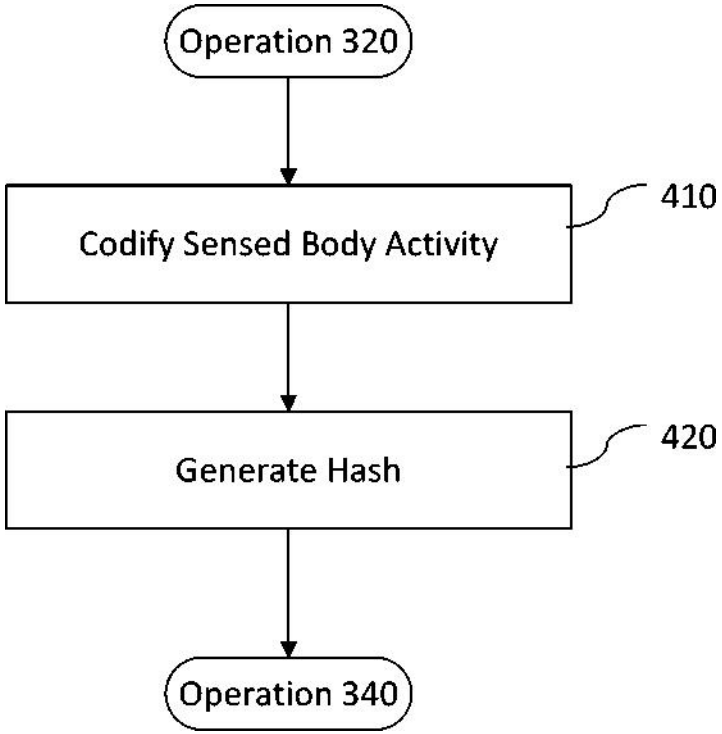
厂320。

3
QO。

生成 BodyActivity 数据。

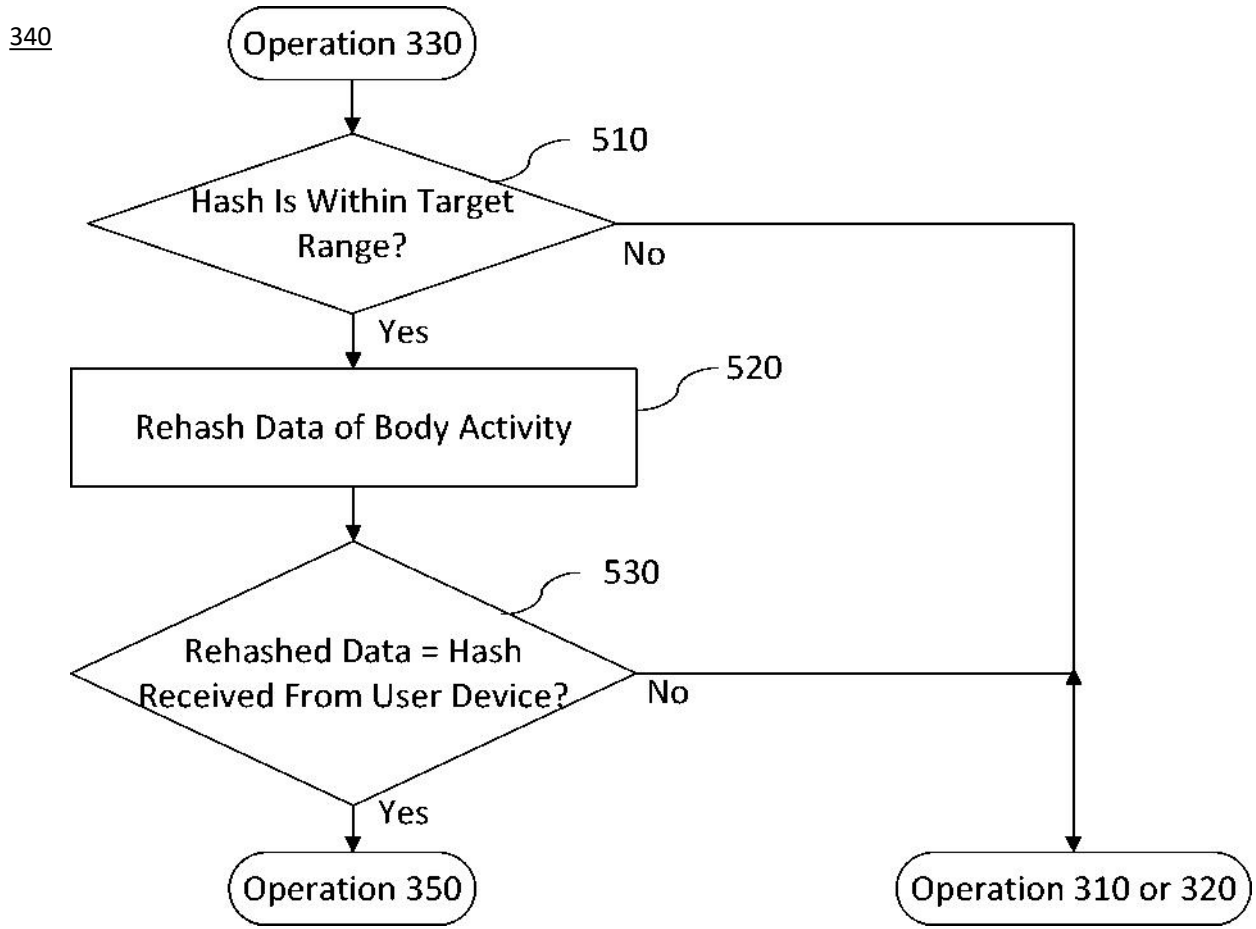


330

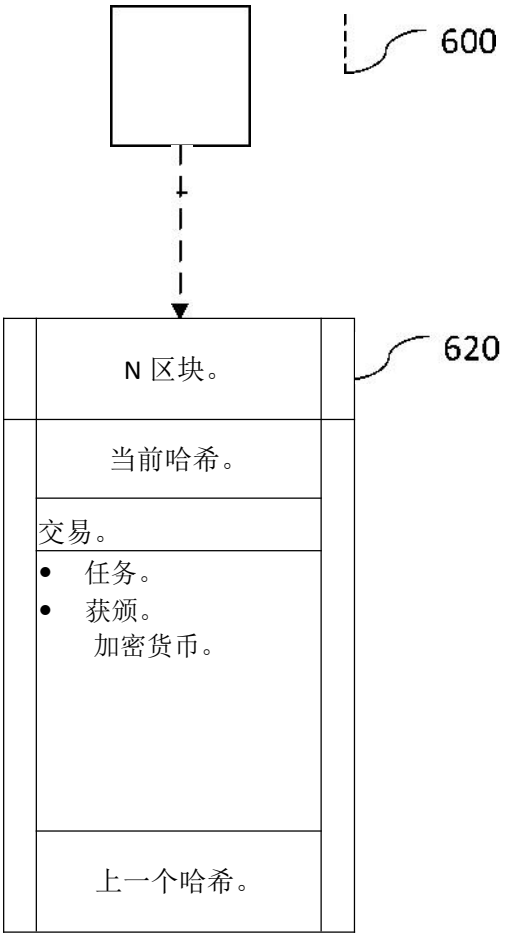

Operation 320
Codify Sensed Body Activity
410
Generate Hash
420
Operation 340

478

插图。4


340
Operation 330
510
Hash Is Within Target Range?
No
Yes
520
Rehash Data of Body Activity
530
Rehashed Data = Hash Received From User Device?
No
Yes
Operation 350
Operation 310 or 320

插图。5



块(N-l)。

当前哈希。

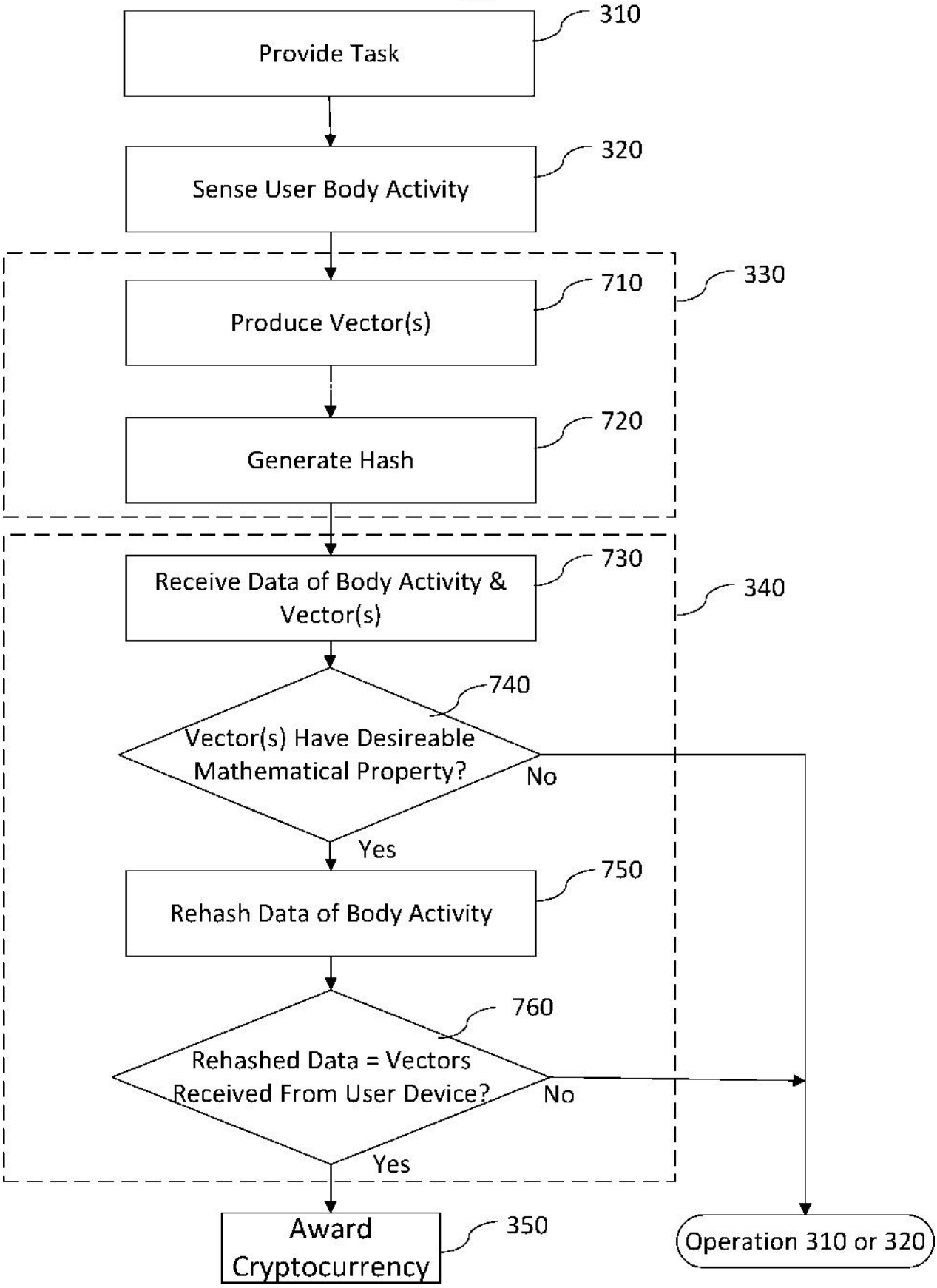
678

交易。

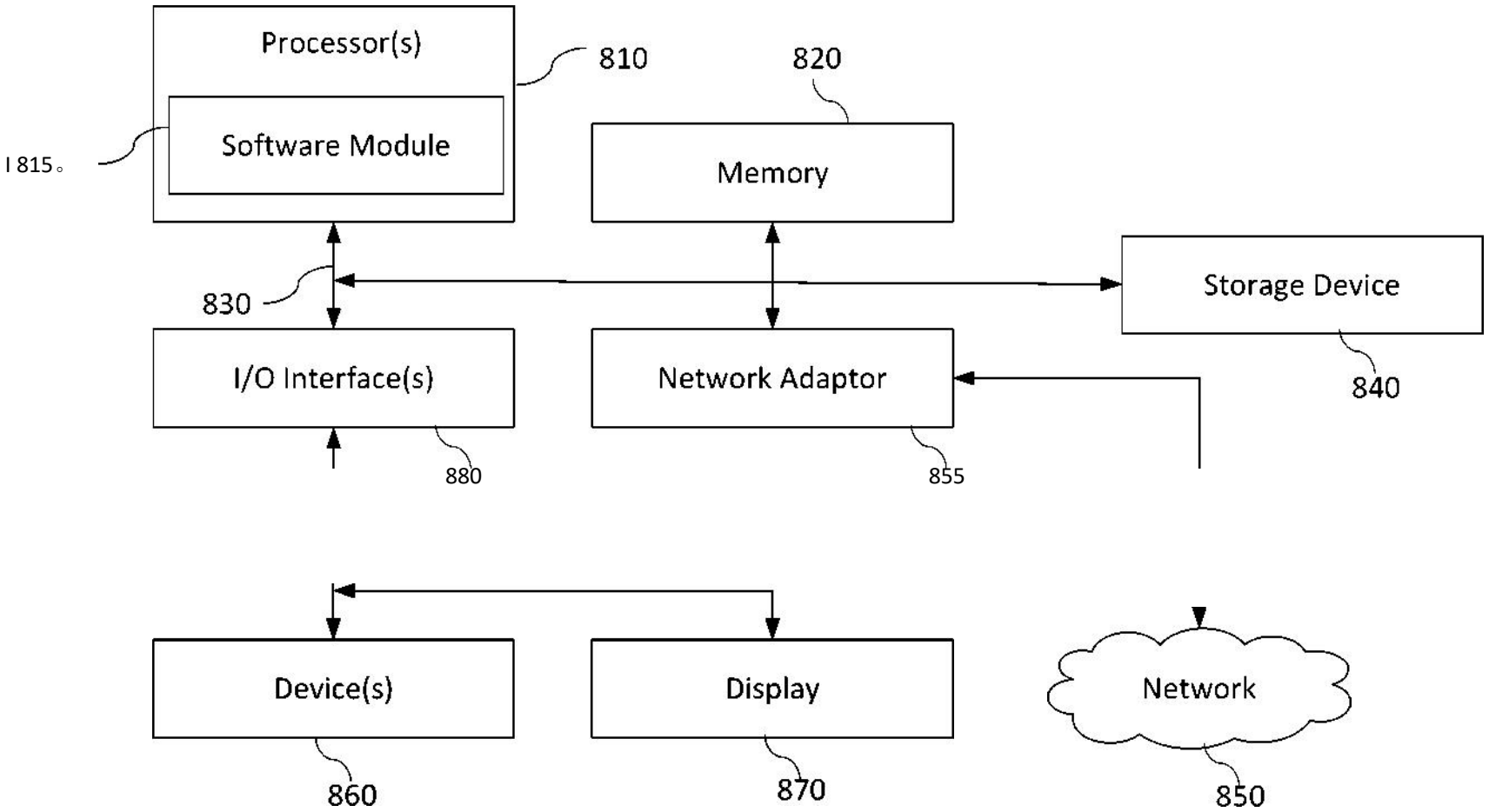
- 任务。
- 获颁。
  加密货币。

上一个哈希。

插图。6


Provide Task
310
Sense User Body Activity
320
330
Produce Vector(s)
710
Generate Hash
720
340
Receive Data of Body Activity & Vector(s)
730
Vector(s) Have Desireable Mathematical Property?
740
No
Yes
Rehash Data of Body Activity
750
Rehashed Data = Vectors Received From User Device?
760
No
Yes
Award Cryptocurrency
350
Operation 310 or 320

插图。7



插图。8

国际搜索报告。

国际申请号。

%/美国 2019/038084。

A.主题分类。

Inv.。G06Q20/O6 G06Q20/32 H04L9/32 G06Q30/02 G06N3/08。

添加。

根据国际专利分类(IPC)或同时根据国家分类和 IPC。

B.搜索的字段。

搜索的最少文档(分类系统后跟分类符号)。

G06Q H04L G07G G06N。

搜索的文档(最低文档除外)，前提是此类文档包括在搜索的字段中。

国际检索期间查阅的电子数据库(数据库名称和可行时使用的检索词)。

EPO-内部，WPI 数据。

C.被视为有关的文件。

类别*。	引述文件，并在适当情况下注明有关段落。	与索赔编号相关。
X。	NeURoress et AL：“通过神经接口 NeURoGRESS 实现机电系统控制”， 2018 年 2 月 8 日(2018-02-08)，XP055612926，从互联网检索： 网 址 ： icostar-Https://s3.eu-centRal-1.amAzonaws.com/ 。 白 皮 书 /d525e659fddaebcl18647 4abc02142360577982f85787dl086372blf0668f4c O.pdf。 [检索于 2019-08-14]。 整个文档。	1-15。

|X|其他文件列在框 C 的后续部分。|X|参见专利族附件。

*引用文件的特殊类别：

“ ”
定义不被认为是支持本发明的原理或理论的本领域总体状况的文件。

具有特别的相关性 11 ‘’ 。
“E”之前的我申请或专利，但在特别相关的国际“X”文件上或之后发表：要求保护的发明不能
“LING DATE 被认为是新奇的或不能被认为包含有创造性的。
“L”单据，该单据可能会对优先权要求提出质疑，或者当单据单独执行时，哪一步是步骤。
引用 t？确定另一个引文或其他特别相关的丫文档的发表日期：要求保护的发明不能。
特殊原因(如指定的)被认为涉及文件在以下情况下的创造性步骤。
“O”文件是指口头披露、使用、展览或其他与一个或多个其他此类文件结合的文件，这种组合。
意味着对一个精通这一领域的人来说是显而易见的。
在国际申请日之前但晚于国际申请日发布的“P”文件。
要求保护同一专利族的文档成员的优先权日期。

在国际申请日期或优先权之后发布的“T”以后的文件。
。日期，并且与申请没有冲突，但引用是为了理解。

实际完成国际搜索的日期。	国际检索报告邮寄日期。
2019 年 8 月 14 日。	2019 年 08 月 27 日。
ISA/的名称和邮寄地址。 欧洲专利局，P.B.。5818 Patentlaan 2 NL-2280 HV Rijswjk 电话：(+31-70)340-2040，传真：(+31-70)340-3016。	获授权人员。 厄尔津·维希(Veshi，Erzim)。

1

表格 PCT/ISA/210(第二页)(2005 年 4 月)。

国际搜索报告。

国际申请号。

%/美国 2019/038084。

C(续)。被视为有关的文件。

类别*。	引述文件，并在适当情况下注明有关段落。	与索赔编号相关。
X。	丽莎·巴里克：“研究人员帮助数字货币用户通过锻炼获得更多奖励”， 2017 年 8 月 14 日(2017-08-14)，XP055613045，从互联网检索： 网址：https://warwick.ac.uk/newsandevents/pr essrelease/Research_Help_Digitai/[检索于 2019-08-14]-。 整个文档。 US 2018 年/247191 Al(Katz Randall M[US]et AL)2018 年 8 月 30 日(2018 年 8 月 8 日至 30 日)第[0069]段-第[0124]段。	1-15。
一个。		1-15。

表格 PCT/ISA/210(续第二页)(2005 年 4 月)。

国际搜索报告。

关于专利家族成员的信息。

国际申请号。

%/美国 2019/038084。

检索报告中引用的专利文献。	出版日期。	专利家族成员。	出版日期。
美国 2018247191。	30-08-2018。	美国 2018247191。	30-08-2018。
		美国 2018341861。	29-11-2018。
		美国 2018373983。	27-12-2018。
		美国 2018373984。	27-12-2018。

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 March 2020 (26.03.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/060606 A1

(51) International Patent Classification:
G06Q 20/06 (2012.01) *G06Q 30/02* (2012.01)
G06Q 20/32 (2012.01) *G06N 3/08* (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2019/038084

(22) International Filing Date:
20 June 2019 (20.06.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/138,518 21 September 2018 (21.09.2018) US

(71) Applicant: **MICROSOFT TECHNOLOGY LICENSING, LLC** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: **ABRAMSON, Dustin**; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **FU, Derrick**; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **JOHNSON, Joseph Edwin, JR.**; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(74) Agent: **MINHAS, Sandip S.** et al.; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) Title: CRYPTOCURRENCY SYSTEM USING BODY ACTIVITY DATA

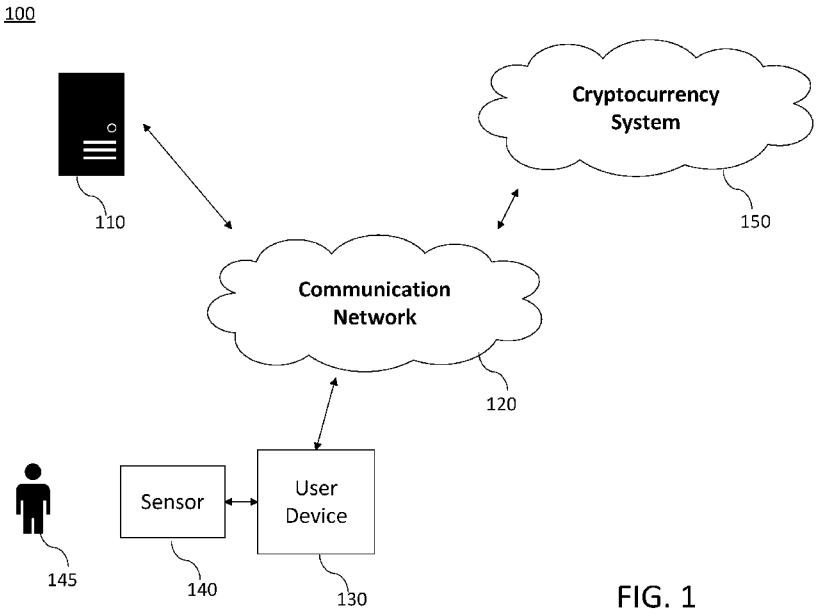


FIG. 1

(57) Abstract: Human body activity associated with a task provided to a user may be used in a mining process of a cryptocurrency system. A server may provide a task to a device of a user which is communicatively coupled to the server. A sensor communicatively coupled to or comprised in the device of the user may sense body activity of the user. Body activity data may be generated based on the sensed body activity of the user. The cryptocurrency system communicatively coupled to the device of the user may verify if the body activity data satisfies one or more conditions set by the cryptocurrency system, and award cryptocurrency to the user whose body activity data is verified.

WO 2020/060606 A1

[Continued on next page]

SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

CRYPTOCURRENCY SYSTEM USING BODY ACTIVITY DATA

BACKGROUND

[0001] A virtual currency (also known as a digital currency) is a medium of exchange implemented through the Internet generally, not tied to a specific government-backed "flat" (printed) currency such as the U.S. dollar or the Euro, and typically designed to allow instantaneous transactions and borderless transfer of ownership. One example of virtual currency is cryptocurrency, wherein cryptography is used to secure transactions and to control the creation of new units.

[0002] Several cryptocurrencies exist. Among these, the most well known is a blockchain-based cryptocurrency. Most blockchain-based cryptocurrency is decentralized in the sense that it has no central point of control. However, blockchain-based cryptocurrency can also be implemented in a centralized system having a central point of control over the cryptocurrency. Bitcoin is one of the examples of blockchain-based cryptocurrency. It is described in a 2008 article by Satoshi Nakamoto, named "Bitcoin: A peer-to-Peer Electronic Cash System".

[0003] A blockchain is a data structure that stores a list of transactions and can be thought of as a distributed electronic ledger that records transactions between source identifier(s) and destination identifier(s). The transactions are bundled into blocks and every block (except for the first block) refers back to or is linked to a prior block in the blockchain. Computer resources (or nodes, etc.) maintain the blockchain and cryptographically validate each new block and the transactions contained in the corresponding block. This validation process includes computationally solving a difficult problem that is also easy to verify and is sometimes called a "proof-of-work". This process is referred to as "mining". The mining may be a random process with low probability so that a lot of trial and error is required to solve a computationally difficult problem. Accordingly, the mining may require enormous amounts of computational energy.

[0004] It is with respect to these and other general considerations that the following embodiments have been described. Also, although relatively specific problems have been discussed, it should be understood that the embodiments should not be limited to solving the specific problems identified in the background.

SUMMARY

[0005] Some exemplary embodiments of the present disclosure may use human body activity associated with a task provided to a user as a solution to "mining" challenges in

cryptocurrency systems. For example, a brain wave or body heat emitted from the user when the user performs the task provided by an information or service provider, such as viewing advertisement or using certain internet services, can be used in the mining process. Instead of massive computation work required by some conventional cryptocurrency systems, data generated based on the body activity of the user can be a proof-of-work, and therefore, a user can solve the computationally difficult problem unconsciously. Accordingly, certain exemplary embodiments of the present disclosure may reduce computational energy for the mining process as well as make the mining process faster.

[0006] Systems, methods, and hardware aspects of computer readable storage media are provided herein for a cryptocurrency system using human body activity data. According to various embodiments of the present disclosure, a server may provide a task to a device of a user which is communicatively coupled to the server. A sensor communicatively coupled to or comprised in the device of the user may sense body activity of the user. Body activity data may be generated based on the sensed body activity of the user. A cryptocurrency system communicatively coupled to the device of the user may verify whether or not the body activity data satisfies one or more conditions set by the cryptocurrency system, and award cryptocurrency to the user whose body activity data is verified.

[0007] Examples are implemented as a computer process, a computing system, or as an article of manufacture such as a device, computer program product, or computer readable medium. According to one aspect, the computer program product is a computer storage medium readable by a computer system and encoding a computer program comprising instructions for executing a computer process.

[0008] This summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Various embodiments in accordance with the present disclosure will be described with reference to the drawings, in which:

[0010] FIG. 1 illustrates an example environment in which some exemplary embodiments of the present disclosure may be practiced;

[0011] FIG. 2 shows a system diagram of a decentralized cryptocurrency system according

to an exemplary embodiment of the present disclosure;

[0012] FIG. 3 shows a flow diagram of a computer-implemented method according to an exemplary embodiment of the present disclosure;

[0013] FIG. 4 shows a flow diagram of an operation for generating body activity data according to an exemplary embodiment of the present disclosure;

[0014] FIG. 5 shows a flow diagram of an operation for verifying body activity data according to an exemplary embodiment of the present disclosure;

[0015] FIG. 6 illustrates a blockchain and two exemplary blocks of the blockchain according to an exemplary embodiment of the present disclosure;

[0016] FIG. 7 shows a flow diagram of a computer-implemented method using a vector or embedding according to another exemplary embodiment of the present disclosure; and

[0017] FIG. 8 illustrates an exemplary block diagram of a computer or processing system in which processes involved in the system, method, and computer program product described herein may be implemented.

[0018] Corresponding numerals and symbols in the different figures generally refer to corresponding parts unless otherwise indicated. The figures are drawn to clearly illustrate the relevant aspects of the embodiments and are not necessarily drawn to scale.

DETAILED DESCRIPTION OF EMBODIMENTS

[0019] In the following detailed description, reference is made to the accompanying drawings which form a part hereof, and in which are shown by way of illustration specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that structural, logical and electrical changes may be made without departing from the spirit and scope of the invention. The following detailed description is therefore not to be taken in a limiting sense, and the scope of the invention is defined only by the appended claims and equivalents thereof. Like numbers in the figures refer to like components, which should be apparent from the context of use.

[0020] The term "cryptocurrency" may mean a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds. Many cryptocurrencies include the use of a blockchain to provide security and prevent fraud as double spending. Some embodiments of the present disclosure may be used in alternate cryptocurrency mechanisms other than a blockchain. The system, method, and computer program products described herein may be applied to both centralized and

decentralized cryptocurrency networks or databases.

[0021] FIG. 1 illustrates an example environment 100 in which some exemplary embodiments of the present disclosure may be practiced. The example environment 100 includes, but is not limited to, at least one of task server 110, communication network 120, user device 130, sensor 140, and cryptocurrency system 150.

[0022] Task server 110 may provide one or more tasks to user device 130 over communication network 120. For example, task server 110 may be at least one of a web server delivering or serving up web pages, an application server handling application operations between users and applications or databases, a cloud server, a database server, a file server, a service server, a game server implementing games or services for a game, and a media server delivering media such as streaming video or audio. The tasks provided by task server 110 will be discussed in more detail below.

[0023] Alternatively, cryptocurrency system 150 may provide one or more tasks to user device 130. For example, in a decentralized cryptocurrency network, the tasks may be proposed to user device 130 by miners (e.g. compute resources or nodes 210 of FIG. 2). In another example, in a centralized cryptocurrency system, a cryptocurrency server may send the tasks to user device 130.

[0024] Communication network 120 may include any wired or wireless connection, the internet, or any other form of communication. Although one network 120 is identified in FIG. 1, communication network 120 may include any number of different communication networks between any of the server, devices, resource and system shown in FIGS. 1 and 2 and/or other servers, devices, resources and systems described herein. Communication network 120 may enable communication between various computing resources or devices, servers, and systems. Various implementations of communication network 120 may employ different types of networks, for example, but not limited to, computer networks, telecommunications networks (e.g., cellular), mobile wireless data networks, and any combination of these and/or other networks.

[0025] User device 130 may include any device capable of processing and storing data/information and communicating over communication network 120. For example, user device 130 may include personal computers, servers, cell phones, tablets, laptops, smart devices (e.g. smart watches or smart televisions). An exemplary embodiment of user device 130 is illustrated in FIG. 6.

[0026] Sensor 140 may be configured to sense the body activity of user 145. As illustrated in FIG. 1, sensor 140 may be a separate component from user device 130 and be operably

and/or communicatively connected to user device 130. Alternatively, sensor 140 may be included and integrated in user device 130. For example, user device 130 may be a wearable device having sensor 140 therein. The sensor 140 may transmit information/data to user device 130. Sensor 140 may include, for example, but not limited to, functional magnetic resonance imaging (fMRI) scanners or sensors, electroencephalography (EEG) sensors, near infrared spectroscopy (NIRS) sensors, heart rate monitors, thermal sensors, optical sensors, radio frequency (RF) sensors, ultrasonic sensors, cameras, or any other sensor or scanner that can measure or sense body activity or scan human body. For instance, the fMRI may measure body activity by detecting changes associated with blood flow. The fMRI may use a magnetic field and radio waves to create detailed images of the body (e.g. blood flow in the brain to detect areas of activity). The material (http://news.berkely.edu/2011/09/22/brain-movies/) shows one example of how the fMRI can measure brain activity associated with visual information and generate image data.

[0027] Cryptocurrency system 150 may include one or more processors for processing commands and one or more memories storing information in one or more cryptocurrency data structures. In some embodiments, cryptocurrency system 150 may be a centralized cryptocurrency system or network, for example, but not limited to, a server which may be privately run by a third party entity or the same entity that is running the task server 110. In other embodiments, cryptocurrency system 150 may be a publically accessible network system (e.g., a distributed decentralized computing system).

[0028] For example, cryptocurrency system 150 may be a decentralized network 200, such as a decentralized blockchain network, including one or more compute resources 210, as shown, for example, in FIG. 2. In the embodiment of FIG. 2, there may be no central authority controlling cryptocurrency network 200. The data stored on blockchain network 200, i.e., the public ledger, may not be stored at a central location in its entirety. Blockchain network 200 may include a plurality of processors for processing commands and a plurality of memories storing information in one or more blockchain data structures. Blockchain network 200 may maintain one or more blockchains of continuously growing lists of data blocks, where each data block refers to previous blocks on its list. The requirement for each block to refer to all previous blocks in the blockchain, yields a chain of blocks that is hardened against tampering and revision, such that the information stored in the blockchain is immutable.

[0029] Compute resources 210 may include any device, computer, system or otherwise that has joined blockchain network 200 and forms a node in blockchain network 200. Compute

resources 210 may include, for example, but not limited to, personal computers, servers, cell phones, tablets, laptops, smart devices (e.g. smart watches or smart televisions), or any other device capable of storing information and communicating over communication network 120. In some embodiments, compute resources 210 may be unaffiliated with or unknown to each other where, for example, compute resources 210 remain anonymous. Each compute resource 210 may include memory 220 that stores a copy of at least a portion of public ledger 230 of blockchain network 200. Compute resources 210 may also execute one or more programs to perform various functions associated with maintaining blockchain network 200 including, for example, updating public ledger 230, generating new blocks, or any other similar function.

[0030] For illustration purposes, FIG. 1 illustrates user device 130 as not included in blockchain network 200. However, user device 130 may be part of blockchain network 200 and be implemented as one of the compute resources 210 in FIG. 2.

[0031] Public ledger 230 may store any transactions performed over blockchain network 200 including but not limited to, for example, any transaction related to and occurring on blockchain network 200. Because each compute resource 210 stores a copy of at least a portion of the public ledger 230 of blockchain network 200, public ledger 230 may be independently verified for accuracy at any time by comparing the stored copies of multiple compute resources 210.

[0032] Communication between compute resources 210 may occur via communication network 120. Communication network 120 of FIG. 2 may be the same network as, or be a different network from, communication 120 of FIG. 1. In some embodiments, each compute resource 210 may communicate directly with each other compute resource 210. In some embodiments, some compute resources 210 may not be able to communicate directly with each other. For example, they are not connected to the same communications network 120. In this case, communications related to blockchain network 200 between the compute resources 210 may occur by using one or more of the remaining compute resources 210 as an intermediary. In some embodiments, one or more of compute resources 210 may not maintain a continuous connection to blockchain network 200 at all times. For example, a compute resource 210 may only be connected to blockchain network 200 during a certain period of time each day or may only be connected to blockchain network 200 intermittently throughout the day. Due to the decentralized nature of blockchain network 200, such an intermittent connection by one or more compute resources 210 does not affect the overall operation of blockchain network 200 since copies of public ledger 230 are stored on multiple

compute resources 210. Once the disconnected compute resource 210 reconnects to blockchain network 200, the disconnected compute resource 210 may receive updated copies of the public ledger 210 from one or more of the compute resources 210 that have been connected to blockchain network 200.

[0033] FIG. 3 shows a flow diagram of a computer-implemented method according to an exemplary embodiment of the present disclosure.

[0034] Method 300 begins at operation 310 illustrated in FIG. 3, where task server 110 provides one or more tasks to device 130 of user 145 over communication network 120. The tasks include, for example, but not limited to, watching or listening information (e.g. advertisement) for a certain time, using services (e.g. search engine, chat bot, e-mail, social media/networking service and any internet or web service), uploading or sending information/data to a website, a server or a network (e.g. content sharing website, and cloud network or server), or any other information or service which may produce effects on users. In the blockchain, the task(s) may be included as a transaction in the public ledger 230.

[0035] Furthermore, the task(s) provided by task server 110 can include solving a test for distinguishing human from machine input so that humans but not computers are able to pass it, such as, Computer Automated Program to Tell Computers and Humans Apart (CAPTCHA) and reCAPTCHA which is a CAPTCHA-like system designed to establish that a computer user is human. The task may require user 145 to solve a verification challenge, for example, but not limited to, an image based challenge including instructions prompting user 145 to solve the challenge through interaction with one or more images.

[0036] At operation 320, when or after user 145 performs the task(s) provided by task server 110, sensor 140 may sense the body activity of user 145 that is a body response related to the task provided by task server 110, and then transmit the sensed body activity of user 145 to user device 130. The body activity may include, for example, but not limited to, radiation emitted from human body, brain activities, body fluid flow (e.g. blood flow), organ activity or movement, body movement, and any other activities that can be sensed and represented by images, waves, signals, texts, numbers, degrees, or any other form of information or data. Examples of body radiation emitted from human body may include radiant heat of the body, pulse rate, or brain wave. Brain waves may comprise, for example, but not limited to, (i) gamma waves, involved in learning or memory tasks, (ii) beta waves, involved in logical thinking and/or conscious thought, (iii) alpha waves, which may be related to subconscious thoughts, (iv) theta waves, which may be related to thoughts involving deep and raw emotions, (v) delta waves, which may be involved in sleep or deep relaxation, or (vi)

electroencephalogram (EEG), which may be measurement used to evaluate the electrical activity in the brain, such as deep concentration. Examples of the body movement may include eye movement, facial movement or any other muscular movements. Furthermore, brain activity can be sensed using the fMRI. The fMRI measures brain activity by detecting changes associated with blood flow. This technique relies on the fact that cerebral blood flow and neuronal activation are coupled. When an area of the brain is in use, blood flow to that region also increases.

[0037] At operation 330, user device 130 generates body activity data based on the body activity sensed by sensor 140. Operation 330 may be part of a mining process which is a process for solving a computationally difficult problem. One exemplary embodiment of operation 330 is shown in FIG. 4. As shown in FIG. 4, operation 330 may comprise operations 410 and 420.

[0038] At operation 410, the body activity sensed by sensor 140 may be codified in symbolic forms, such as letter(s), numeral(s), symbol(s), and a string comprising sequence of characters. In one example, the body activity can be codified by extracting one or more values from the sensed body activity, such as minimum and/or maximum amplitude(s) or frequency(ies) of a body activity signal (e.g. brain waves). In another example, user device 130 may window and sample the sensed body activity over time and calculate the average of the sampled values. In still another example, user device 130 may generate raw data of the body activity. In still another example, user device 130 may filter a raw signal of the body activity using one or more filters to apply the filtered body activity signal to an audio hash function or algorithm at operation 420. Alternatively, any statistic value(s) associated with human body activity can be codified from the body activity sensed by sensor 140.

[0039] At operation 420, the codified body activity may be converted into an encrypted output by using an encryption algorithm, such as a hash algorithm or function. For example, hash functions include functions that map an initial input data set of an output data set. Generally, the hash function may be any function that can be used to map data of arbitrary size to data of fixed size. The hash function allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it (or any equivalent alternatives) by knowing the stored hash value. The hash algorithm or function may be included in the mining software or program of the cryptocurrency system or database.

[0040] For example, operation 420 may use audio hash function, where the histogram of frequencies of the codified body activity are summed up, or bit manipulation, such as XOR

function of each histogram bucket with the next or a modulus of a prime number, is performed on the codified body activity.

[0041] In some embodiments, an analog hash function where the body activities themselves are hashes can be used. For example, waves or signals sensed by sensor 140, for example, but not limited to, alpha, beta, delta or gamma waves from the EEG sensor, may be transformed to a histogram using a transforming algorithm or formula, such as Fast Fourier Transform (FFT) or any other algorithm or formula that can convolve, add or multiply waves or signals to produce a histogram. The hash may be the histogram itself. For example, the hash may be the output of the FFT where each component is a frequency band and the value is counts corresponding to each frequency band. In another example, the desired properties may be that the first two frequency histograms are as close to zero as possible, for instance, provided some statistical guarantee exists that this cannot happen easily.

[0042] However, operation 420 is optional. In certain embodiments, user device 130, without encrypting or hashing the codified body activity, may transmit the codified body activity generated at operation 410 to cryptocurrency system 150.

[0043] Although FIG. 3 illustrates that operation 330, including operation 410 and 420, is processed by user device 130, at least one of operations 410 and 420 can be processed by another device(s), server, resource or system, such as task server 110, cryptocurrency system 150 or any other server. For example, the user device 130 may generate raw data of the sensed body activity, transmit it to cryptocurrency system 150, task server 110 or any other server, and then cryptocurrency system 150, task server 110 or any other server may codify or hash the raw data of the sensed body activity.

[0044] Referring back to FIG. 3, at operation 340, cryptocurrency system 150 verifies if the body activity data of user 145 generated by user device 130 satisfies one or more conditions set by an algorithm of cryptocurrency system 150. The conditions may be set by simulating human body activity across all of body activities that can constitute hashes. Machine learning algorithms may be used to simulate body activities and set the conditions for valid body activities, for example, but not limited to, using generative adversarial networks.

[0045] In some embodiments, cryptocurrency system 150 verifies whether the body activity data of user 145 (e.g. the code of the body activity generated at operation 410 or the hash of the body activity generated at operation 420) may represent that the body activity of user 145 is within a target range. The target range may be determined using the amount of cognitive effort that user 145 requires to perform the task provided by task server 110. For example, to verify if the hash of the body activity of user 145, cryptocurrency system 150

may determine, for example, but not limited to, (i) whether the hash of the body activity of user 145 has a specific certain pattern, repeated patterns, a mathematical properties or the number of leading numbers, characters or strings (e.g. leading zeroes) set by cryptocurrency system 150, or (ii) whether the hash of the body activity of user 145 is less than a current target value. Examples of the numerical patterns set by cryptocurrency system 150 may be a pattern that first certain digits of the hash form a prime number, or a pattern that a number that is calculated by applying first certain digits of the hash to a preset formula forms a prime number (For example, a number calculated by adding or subtracting a predetermined number or a number set by cryptocurrency system 150 to the first four digits of the hashing forms a prime number). The repeating number patterns may include a repeating number (e.g. leading zeros, ones in the middle of the hash, twos in the last four digits of the hash, and any repeating numbers included in the hash) and a repeating number sequence (e.g. leading repeating digit pairs, such as "121212", or triplets "123123"). If the hash of the body activity of user 145 has the desirable pattern(s) or is within the target range, then the proof of work or proof of stake is considered solved, and that hash can be a new block. The target range or value may be changed periodically to maintain a preselected level of difficulty, although it is not required. For example, the target value may be inversely proportional to the difficulty. By varying the difficulty, a roughly constant rate of block generation may be kept.

[0046] The target range of valid body activity may be set using statistical data so that normal body activity, activity that can easily happen, or faking body activity cannot be validated. For example, the target range of valid body activity may be selected from a range that human miners cannot fake their own body activity to satisfy the target range to prove and validate the proof-of-work.

[0047] Additionally, the verification at operation 340 may include filtering out invalid tasks, malformed data (syntax errors) or data sent from an unauthorized user or generated by a machine learning system. For example, cryptocurrency system 150 may receive, from user device 130, data of the body activity generated before the hash algorithm is applied, rehash that data, and then compare the rehashed data with the hash received from user device 130 to check whether the body activity data is generated based on human, not random computer generated data. Voxel(s) of the image of the fMRI may be an example of the data of the body activity generated before the hash algorithm is applied.

[0048] One exemplary embodiment of operation 340 is shown in FIG. 5. At operation 510, cryptocurrency system 150 may check whether the hash of the body activity, received from

user device 130, is within the target range set by cryptocurrency system 150, or comprises a desirable pattern set by cryptocurrency system 150. If the hash of the body activity is within the target range or has a desirable pattern set by cryptocurrency system 150, cryptocurrency system 150 rehashes data of the body activity, generated before the hash algorithm is applied and transmitted with the hash of the body activity from user device 130 (Operation 520), and then compare the rehashed data with the hash of the body activity, received from user device 130 (Operation 530). If the rehashed data is identical to the hash of the body activity, received from user device 130, cryptocurrency system 150 proceeds to operation 350. However, if determining in operation 510 that the hash of the body activity data is out of the target range or does not include the desirable pattern set by cryptocurrency system 150 or if determining in operation 530 that the rehashed data does not match the hash of the body activity, operation 310 or 320 may be proceeded.

[0049] At operation 350, when the body activity data transmitted from user device 130 satisfies one or more conditions set by cryptocurrency system 150, cryptocurrency system 150 awards cryptocurrency to user 145. For example, cryptocurrency system 150 awards to user 145 an amount of cryptocurrency corresponding to the task accomplished by user 145. Additionally, cryptocurrency system 150 may award cryptocurrency to an owner or operator of task server 110 as a reward for providing services, such as, search engines, chatbots, applications or websites, offering users access for free to paid contents (e.g. video and audio streaming or electric books), or sharing information or data with users.

[0050] For example, in the blockchain cryptocurrency system, at operation 340, at least one of compute resources 210 of FIG. 2 verifies if the hash of the body activity data of user 145 is valid. At operation 350, when the hash of the body activity data of user 145 is validated at operation 340, the compute resource 210 of FIG. 2 can add a new block to the blockchain. The new block may contain the number of cryptocurrency units assigned to the user's address. The new blockchain with the additional added block is broadcasted around the cryptocurrency network 150. The compute resource 210, which performed operations 340 and 350, may be also rewarded with transaction fees and/or cryptocurrency.

[0051] FIG. 5 depicts a blockchain 500 and two exemplary blocks 510, 520 of blockchain 500 according to exemplary embodiments of the present disclosure. Typically a "blockchain" is understood as being a data structure comprising a series of blocks, where each block includes data corresponding to one or more transactions, hashed together with linking data, such as the hash of an immediately preceding block. In the embodiment of the present disclosure, the transaction may be the task performed by user 145. The chain can

then be used to create a ledger, which is typically an append-only database. Once data is entered into a block of the chain, the entry is essentially irrefutable, since any tampering with the data would be reflected in the chained hash calculations and is thus easily detected.

[0052] The blockchain 500 may represent the publicly distributable transactions ledger, such as ledger 230 of FIG. 2, and may include a plurality of blocks. Each block, such as block 510 and block 520 may include data regarding recent transactions. For example, the task performed by user 145 and the number of cryptocurrency units awarded to user 145, and/or contents linking data that links one block 520 to a previous block 510, and proof-of-work data, for example, the validated hash of the body activity, that ensures that the state of the blockchain 500 is valid and is endorsed/verified by a majority of the record keeping system. Exemplary embodiments of block 520 of blockchain 500 may include a current hash, a previous hash of previous block 510, transaction. The previous hash is a hash from the immediately preceding block, which ensures that each block is immutably tied to previous block. The hash of previous block 510 may be included in block 520, thereby linking block 520 to previous block 510.

[0053] Transaction information cannot be modified without at least one of compute resources 210 noticing, thus, the blockchain 500 can be trusted to verify transactions occurring on blockchain 500.

[0054] In some embodiments, vectors or embeddings may be used for body activity data. FIG. 7 shows a flow diagram of an exemplary embodiment of a computer-implemented method using vectors (or embedding). As described in detail above with respect to FIG. 3, task server 110 or cryptocurrency system/network 150, such as a central cryptocurrency server or compute resource (or node) 210, may perform operation 310 where one or more tasks are proposed to user device 130 over communication network 120, and sensor 140 may perform operation 320 where sensor 140 senses or measures the body activity of user 145. Sensor 140 (or user device 130) may generate data of the body activity in the form of images, waves, signals, numbers, characters, strings or any other form that can represent the body activity.

[0055] At operation 710, user device 130 produces one or more vectors (or embeddings), such as an array of floating point numbers, from the data of the body activity generated by sensor 140 (or user device 130). An algorithm stored in user device 130, or any device, server, system or network communicatively connected to user device 130 over communication network 120, may transform the data of the body activity generated by sensor 140 (or user device 130) into one or more vectors. For example, the brain image

generated by the fMRI scanner may be fed into a computer vision machine learning algorithm, for example, but limited to, a convolution neural network, and the machine learning algorithm may generate one or more vectors from one or more voxels of the brain image. In some embodiments, one single vector may be generated at operation 710. In other embodiments, a series of vectors may be produced by sampling over time when user 145 is performing the task(s). The data of the body activity (e.g. voxels of a brain image) and/or the vectors (or embeddings) may generate a "proof of work" and be transmitted to cryptocurrency system/network 150.

[0056] In addition, the vectors may optionally include one or more vectors related to the task(s), for example, but not limited to, search terms that user 145 used or identifier(s) of advertisement that user 145 viewed.

[0057] At operation 720, the vector(s) generated at operation 710 may be converted into an encrypted output by using an encryption algorithm, such as a hashing algorithm or function, as explained above with respect to operation 420 of FIG. 4. For example, the vector(s) can be hashed as bytes with the hashing algorithm, such as Secure Hash Algorithm (SHA)-1, SHA-256, SHA-384, SHA-512, and Message Digest (MD)-5.

[0058] However, operation 720 is optional. In some embodiments, user device 130 can transmit the vector(s) of the body activity produced at operation 710 to cryptocurrency system 150 without encrypting or hashing them.

[0059] At operation 730, cryptocurrency system 150 receives, from user device 130, the data of the body activity of user 145 (e.g. voxels of a brain image) and/or the vector(s) (or the hash) of the body activity of user 145.

[0060] At operation 740, cryptocurrency system 150 checks if the vector(s) received from user device 130 have one or more mathematical properties set by cryptocurrency system/network 150. For example, cryptocurrency system 150 may determine whether the vector(s) of the body activity have similarity (or relationship) with a legitimate vector (or a baseline vector) set by an algorithm of cryptocurrency system 150. The similarity may be measured or calculated using, for example, but not limited to, a cosine similarity, the Euclidean distance, the Manhattan distance, the Minkowski distance, and the Jaccard similarity. The legitimate vector may be set based on the assumption that the vectors of body activities of people who are performing the same task have a certain degree of similarity. Cryptocurrency system 150, such as a central cryptocurrency server/network or compute resource (or node) 210 of FIG. 2, can decide the legitimate vector and similarity. For example, miners like compute resources (or nodes) 210 of FIG. 2 can share their proof

of work including, for example, but not limited to, vectors of body activities, with cryptocurrency network 150, and decide the legitimate vector and similarity by calculating the average of the proof of work (e.g. a centroid or weighted average of the vectors and a standard deviation).

[0061] If the vector(s) received from user device 130 have the mathematical property(ies) set by cryptocurrency system/network 150, cryptocurrency system/network 150 rehashes the data of the body activity, transmitted from user device 130 (Operation 750), and then compares the rehashed output with the vectors (or the hash) received from user device 130 (Operation 760). For example, computer resource (or node) 210 of FIG. 2 may rehash the fMRI voxels, transmitted from user device 130, to a vector, and then compare the rehashed vector with the vector received from user device 130 to check whether the body activity data is generated based on human, not random computer generated data. If determining in operation 740 that the vector(s) received user device 130 do not satisfy the mathematical property(ies) set by cryptocurrency system/network 150 or if determining in operation 760 that the rehashed output does not match the vector(s) (or the hash) received from user device 130, operation 310 or 320 may be proceeded.

[0062] If the rehashed output is identical to the vector(s) (or the hash) received from user device 130, cryptocurrency system/network 150 awards cryptocurrency to user 145 as described in detail above with respect to operation 350. For example, in the blockchain cryptocurrency system, a miner, such as one of compute resources (or nodes) 210 of FIG. 2, which performed the validation of the body activity data, may add a new block, which includes the data of the body activity, the vector(s) (or the hash) and/or the number of cryptocurrency units assigned to the user's address, to the blockchain, broadcast a new blockchain with the new block around cryptocurrency network 150, and may be rewarded with transaction fees and/or cryptocurrency.

[0063] FIG. 8 illustrates a schematic of an example computer or processing system that may implement any of the systems, methods, and computer program products, such as task server 110, user device 130, cryptocurrency system 150 and compute resources 210, described herein in one embodiment of the present disclosure. The computer system is only one example of a suitable processing system and is not intended to suggest any limitation as to the scope of use or functionality of embodiments of the methodology described herein. The processing system shown may be operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well-known computing systems, environments, and/or configurations that may be suitable for use

with the processing system shown in FIG. 8 may include, but are not limited to, personal computer systems, server computer systems, thin clients, thick clients, handheld or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputer systems, mainframe computer systems, and distributed cloud computing environments that include any of the above systems or devices, and the like.

[0064] The computer system may be described in the general context of computer system executable instructions, such as program modules, being executed by a computer system. Generally, program modules may include routines, programs, objects, components, logic, data structures, and so on that perform particular tasks or implement particular abstract data types. The computer system may be practiced in distributed cloud computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed cloud computing environment, program modules may be located in both local and remote computer system storage media including memory storage devices.

[0065] The components of computer system 800 may include, but are not limited to, one or more processors or processing units 810, system memory 820, and bus 830 that couples various system components including system memory 820 to processor 810. Processor 810 may include software module 815 that performs the methods described herein. The module 815 may be programmed into the integrated circuits of processor 810, or loaded from memory 820, storage device 840, or network 850 or combinations thereof.

[0066] Bus 830 may represent one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnects (PCI) bus.

[0067] Computer system 800 may include a variety of computer system readable media. Such media may be any available media that is accessible by computer system, and it may include both volatile and non-volatile media, removable and non-removable media.

[0068] System memory 820 can include computer system readable media in the form of volatile memory, such as random access memory (RAM) and/or cache memory or others. Computer system 800 may further include other removable/non-removable volatile/non-

volatile computer system storage media. By way of example only, storage device 840 can be provided for reading from and writing to a non-removable, non-volatile magnetic media (e.g., a "hard drive"). Although not shown, a magnetic disk drive for reading from and writing to a removable, non-volatile magnetic disk (e.g., a "floppy disk"), and an optical disk drive for reading from or writing to a removable, non-volatile optical disk such as a CD-ROM, DVD-ROM or other optical media can be provided. In such instances, each can be connected to bus 630 by one or more data media interfaces.

[0069] Computer system 800 may also communicate with one or more external devices 860 such as a keyboard, a pointing device, a display 870, etc; one or more devices that enable a user to interact with computer system; and/or any devices (e.g., network card, modem, etc.) that enable computer system to communicate with one or more other computing devices. Such communication can occur via Input/Output (I/O) interfaces 880.

[0070] Still yet, computer system 800 can communicate with one or more networks 850 such as a local area network (LAN), a general wide area network (WAN), and/or a public network (e.g., the Internet) via network adapter 855. As depicted, network adapter 855 communicates with the other components of computer system via bus 830. It should be understood that although not shown, other hardware and/or software components could be used in conjunction with computer system. Examples include, but are not limited to: microcode, device drivers, redundant processing units, external disk drive arrays, RAID systems, tape drives, and data archival storage systems, etc.

[0071] As will be appreciated by one skilled in the art, aspects of the present disclosure may be embodied as a system, method or computer program product. Accordingly, aspects of the present disclosure may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit," "module" or "system." Furthermore, aspects of the present disclosure may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.

[0072] Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include

the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

[0073] A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium may be any computer readable medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device.

[0074] Program code embodied on a computer readable medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

[0075] Computer program code for carrying out operations for aspects of the present invention may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages, a scripting language such as Perl, VBS or similar languages, and/or functional languages such as Lisp and ML and logic-oriented languages such as Prolog. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[0076] Aspects of the present disclosure are described with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to some embodiments of the present disclosure. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of

blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0077] These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

[0078] The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0079] The flowchart and block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

[0080] The computer program product may comprise all the respective features enabling the implementation of the methodology described herein, and which - when loaded in a

computer system - is able to carry out the methods. Computer program, software program, program, or software, in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following: (a) conversion to another language, code or notation; and/or (b) reproduction in a different material form.

[0081] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0082] The corresponding structures, materials, acts, and equivalents of all means or step plus function elements, if any, in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present invention has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the invention. The embodiment was chosen and described in order to best explain the principles of the invention and the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

[0083] Various aspects of the present disclosure may be embodied as a program, software, or computer instructions embodied in a computer or machine usable or readable medium, which causes the computer or machine to perform the steps of the method when executed on the computer, processor, and/or machine. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform various functionalities and methods described in the present disclosure is also provided.

[0084] The system and method of the present disclosure may be implemented and run on a general-purpose computer or special-purpose computer system. The terms "computer

system" and "computer network" as may be used in the present application may include a variety of combinations of fixed and/or portable computer hardware, software, peripherals, and storage devices. The computer system may include a plurality of individual components that are networked or otherwise linked to perform collaboratively, or may include one or more stand-alone components. The hardware and software components of the computer system of the present application may include and may be included within fixed and portable devices such as desktop, laptop, and/or server. A module may be a component of a device, software, program, or system that implements some "functionality", which can be embodied as software, hardware, firmware, electronic circuitry, or etc.

[0085] Although specific embodiments of the present invention have been described, it will be understood by those of skill in the art that there are other embodiments that are equivalent to the described embodiments. Accordingly, it is to be understood that the invention is not to be limited by the specific illustrated embodiments, but only by the scope of the appended claims.

CONCEPTS

[0086] Concept 1. A cryptocurrency system, comprising: one or more processors; and memory storing executable instructions that, if executed by the one or more processors, configure the cryptocurrency system to: communicate with a device of a user; receive body activity data which is generated based on body activity of the user, wherein the body activity is sensed by a sensor communicatively coupled to or comprised in the device of the user; verify if the body activity data of the user satisfies one or more conditions set by the cryptocurrency system; and award cryptocurrency to the user whose body activity data is verified.

[0087] Concept 2. The system of any preceding and/or succeeding Concept(s), wherein the body activity sensed by the sensor comprises at least one of body radiation emitted from the user, body fluid flow, a brain wave, pulse rate or body heat radiation.

[0088] Concept 3. The system of any preceding and/or succeeding Concept(s), wherein the one or more conditions are set based on an amount of human body activity associated with a task which is provided to the device of the user.

[0089] Concept 4. The system of any preceding and/or succeeding Concept, wherein the one or more conditions comprise a condition that the body activity data represents that the user performs a task provided to the device of the user.

[0090] Concept 5. The system of any preceding and/or succeeding Concept(s), wherein the body activity data is generated using a hash algorithm converting human body activity into

an encryption output, and the generated body activity data comprises a hash of the sensed body activity of the user.

[0091] Concept 6. The system of any preceding and/or succeeding Concept(s), wherein the body activity data comprises one or more vectors produced from the body activity sensed by the sensor.

[0092] Concept 7. The system of any preceding and/or succeeding Concept(s), wherein the one or more conditions include a condition that the hash of the body activity includes repeated patterns or a mathematical property set by the cryptocurrency system.

[0093] Concept 8. The system of any preceding and/or succeeding Concept(s), wherein the cryptocurrency system awards the cryptocurrency to the user by generating a block for the awarded cryptocurrency and adding the block to a blockchain stored in the cryptocurrency system.

[0094] Concept 9. The system of any preceding and/or succeeding Concept(s), wherein the block comprises data comprising: a task provided to the device of the user; information on the awarded cryptocurrency; a hash associated with the body activity; and a hash of a previous block.

[0095] Concept 10. The system of any preceding and/or succeeding Concept(s), wherein the task provided to the device of the user comprises a test for verifying if the user of the device is human or not.

[0096] Concept 11. The system of any preceding and/or succeeding Concept(s), wherein the cryptocurrency system is configured to: receive, from the device of the user, data of the body activity generated before the hash algorithm is applied and the hash of the body activity; rehash the data of the body activity; and compare the rehashed data with the hash of the body activity received from the device of the user to verify the body activity data.

[0097] Concept 12. A computer-implemented method, comprising: receiving, by a device of a user coupled to a network, a task over the network; sensing, by a sensor communicatively coupled to or comprised in the device of the user, body activity of the user; generating body activity data based on the sensed body activity of the user; verifying, by a cryptocurrency system communicatively coupled to the device of the user, if the body activity data satisfies one or more conditions set by the cryptocurrency system; and awarding, by the cryptocurrency system, cryptocurrency to the user whose body activity data is verified.

[0098] Concept 13. The method of any preceding and/or succeeding Concept(s), wherein the body activity sensed by the sensor comprises at least one of body radiation emitted from

the user, body fluid flow, a brain wave, pulse rate or body heat radiation.

[0099] Concept 14. The method of any preceding and/or succeeding Concept(s), wherein the one or more conditions are set by the cryptocurrency system based on an amount of human body activity associated with the task provided to the device of the user.

[00100] Concept 15. The method of any preceding and/or succeeding Concept(s), wherein the verifying if the body activity data satisfies the one or more conditions comprises determining if the body activity data represents that the user performs the task provided to the device of the user.

[00101] Concept 16. The method of any preceding and/or succeeding Concept(s), wherein the verifying if the body activity data satisfies the one or more conditions comprises determining if the body activity data represents more than an amount of the body activity set by the cryptocurrency system.

[00102] Concept 17. The method of any preceding and/or succeeding Concept(s), wherein the body activity data is generated using a hash algorithm converting human body activity into an encryption output, and the generated body activity data comprises a hash of the sensed body activity of the user.

[00103] Concept 18. The method of any preceding and/or succeeding Concept(s), wherein the body activity data comprises one or more vectors produced from the body activity sensed by the sensor.

[00104] Concept 19. The method of any preceding and/or succeeding Concept(s), wherein the verifying if the body activity data satisfies the one or more conditions set by the cryptocurrency system comprises determining if the hash of the sensed body activity includes repeated patterns or a mathematical property set by the cryptocurrency system.

[00105] Concept 20. The method of any preceding and/or succeeding Concept(s), wherein the awarding the cryptocurrency comprises generating, by the cryptocurrency system, a block for the awarded cryptocurrency and adding the generated block to a blockchain stored in the cryptocurrency system.

[00106] Concept 21. The method of any preceding and/or succeeding Concept(s), wherein the block comprises data comprising: the task provided to the device of the user; information on the awarded cryptocurrency; the generated hash associated with the body activity; and a hash of a previous block.

[00107] Concept 22. The method of any preceding and/or succeeding Concept(s), wherein the task comprises a test for verifying if the user of the device is human or not.

[00108] Concept 23. The method of any preceding and/or succeeding Concept(s),

further comprising: receiving, by the cryptocurrency system, from the device of the user, data of the body activity generated before the hash algorithm is applied and the hash of the body activity; rehashing, by the cryptocurrency system, the data of the body activity; and comparing, by the cryptocurrency system, the rehashed data with the hash of the body activity received from the device of the user to verify the body activity data.

[00109] Concept 24. A device, comprising: one or more processors communicatively coupled to a sensor, the sensor configured to sense body activity of a user; and memory storing executable instructions that, if executed by the one or more processors, configure the device to: receive a task; generate body activity data based on the sensed body activity of the user, wherein the sensed body activity is associated with the received task; and transmit the generated body activity data to a system or network which verifies the body activity data to award cryptocurrency.

[00110] Concept 25. The system of any preceding and/or succeeding Concept(s), wherein the body activity sensed by the sensor comprises at least one of body radiation emitted from the user, body fluid flow, a brain wave, pulse rate or body heat radiation.

[00111] Concept 26. The system of any preceding and/or succeeding Concept(s), wherein the body activity data is generated using a hash algorithm converting human body activity into an encryption output.

[00112] Concept 27. The system of any preceding and/or succeeding Concept(s), wherein the body activity data comprises one or more vectors produced from the body activity sensed by the sensor.

[00113] Concept 28. The system of any preceding and/or succeeding Concept(s), wherein the body activity data is generated by producing one or more vectors from the body activity sensed by the sensor and encrypting the one or more vectors.

CLAIMS

1. A cryptocurrency system, comprising:

one or more processors; and

memory storing executable instructions that, if executed by the one or more processors, configure the cryptocurrency system to:

communicate with a device of a user;

receive body activity data which is generated based on body activity of the user, wherein the body activity is sensed by a sensor communicatively coupled to or comprised in the device of the user;

verify if the body activity data of the user satisfies one or more conditions set by the cryptocurrency system; and

award cryptocurrency to the user whose body activity data is verified.

2. The system of claim 1, wherein the body activity sensed by the sensor comprises at least one of body radiation emitted from the user, body fluid flow, a brain wave, pulse rate or body heat radiation.

3. The system of claim 1, wherein the one or more conditions are set based on an amount of human body activity associated with a task which is provided to the device of the user.

4. The system of one of claims 1-3, wherein the body activity data is generated using a hash algorithm converting human body activity into an encryption output, and the generated body activity data comprises a hash of the sensed body activity of the user.

5. The system of one of claims 1-3, wherein the body activity data comprises one or more vectors produced from the body activity sensed by the sensor.

6. The system of one of claims 1-3, wherein the cryptocurrency system awards the cryptocurrency to the user by generating a block for the awarded cryptocurrency and adding the block to a blockchain stored in the cryptocurrency system.

7. The system of claim 6, wherein the block comprises data comprising:

a task provided to the device of the user;

information on the awarded cryptocurrency;

a hash associated with the body activity; and

a hash of a previous block.

8. The system of claim 3, wherein the task provided to the device of the user comprises a test for verifying if the user of the device is human or not.

9. The system of claim 4, wherein the cryptocurrency system is configured to:

receive, from the device of the user, data of the body activity generated before the hash algorithm is applied and the hash of the body activity;

rehash the data of the body activity; and

compare the rehashed data with the hash of the body activity received from the device of the user to verify the body activity data.

10. A computer-implemented method, comprising:

receiving, by a device of a user coupled to a network, a task over the network;

sensing, by a sensor communicatively coupled to or comprised in the device of the user, body activity of the user;

generating body activity data based on the sensed body activity of the user;

verifying, by a cryptocurrency system communicatively coupled to the device of the user, if the body activity data satisfies one or more conditions set by the cryptocurrency system; and

awarding, by the cryptocurrency system, cryptocurrency to the user whose body activity data is verified.

11. The method of claim 10, wherein the body activity sensed by the sensor comprises at least one of body radiation emitted from the user, body fluid flow, a brain wave, pulse rate or body heat radiation.

12. The method of claim 10, wherein the one or more conditions are set by the cryptocurrency system based on an amount of human body activity associated with the task provided to the device of the user.

13. The method of one of claims 10-12, wherein the body activity data is generated using a hash algorithm converting human body activity into an encryption output, and the generated body activity data comprises a hash of the sensed body activity of the user.

14. The method of one of claims 10-12, wherein the body activity data comprises one or more vectors produced from the body activity sensed by the sensor.

15. The method of claim 13, further comprising:

receiving, by the cryptocurrency system, from the device of the user, data of the body activity generated before the hash algorithm is applied and the hash of the body activity;

rehashing, by the cryptocurrency system, the data of the body activity; and

comparing, by the cryptocurrency system, the rehashed data with the hash of the body activity received from the device of the user to verify the body activity data.

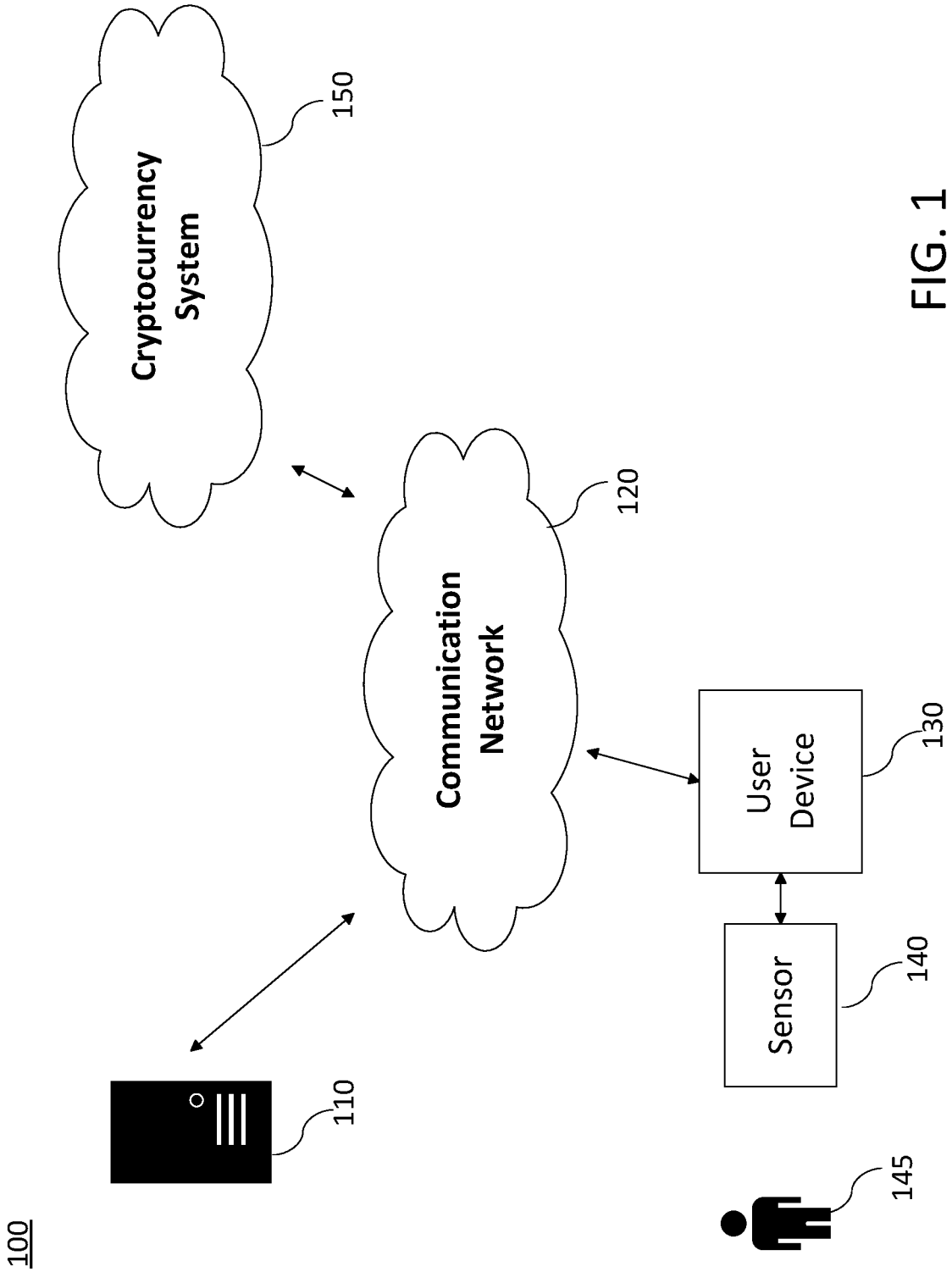

Cryptocurrency System
150
Communication Network
120
User Device
130
Sensor
140
110
145
100

FIG. 1

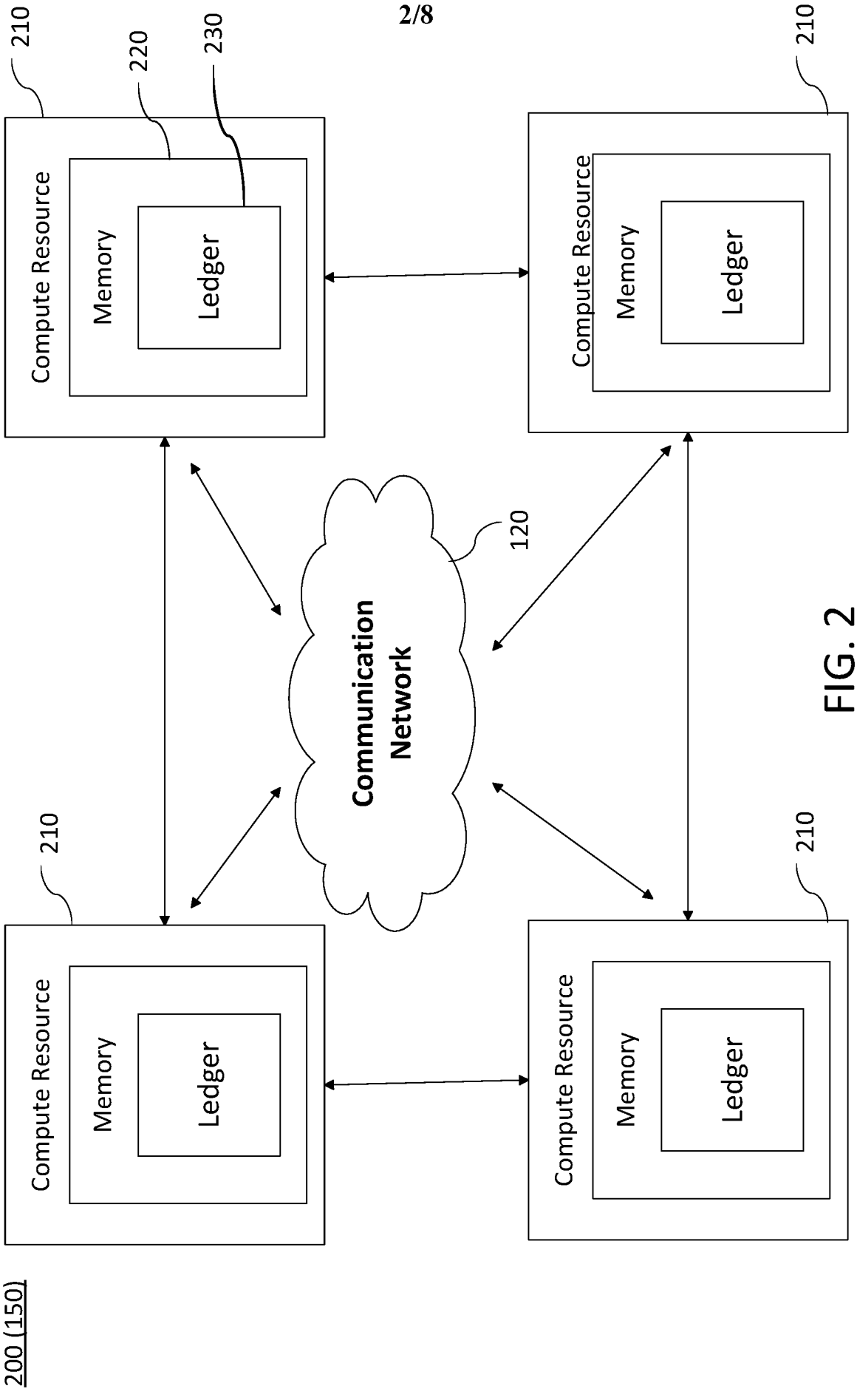

200 (150)
210
220
230
Compute Resource
Memory
Ledger
120
Communication Network

FIG. 2

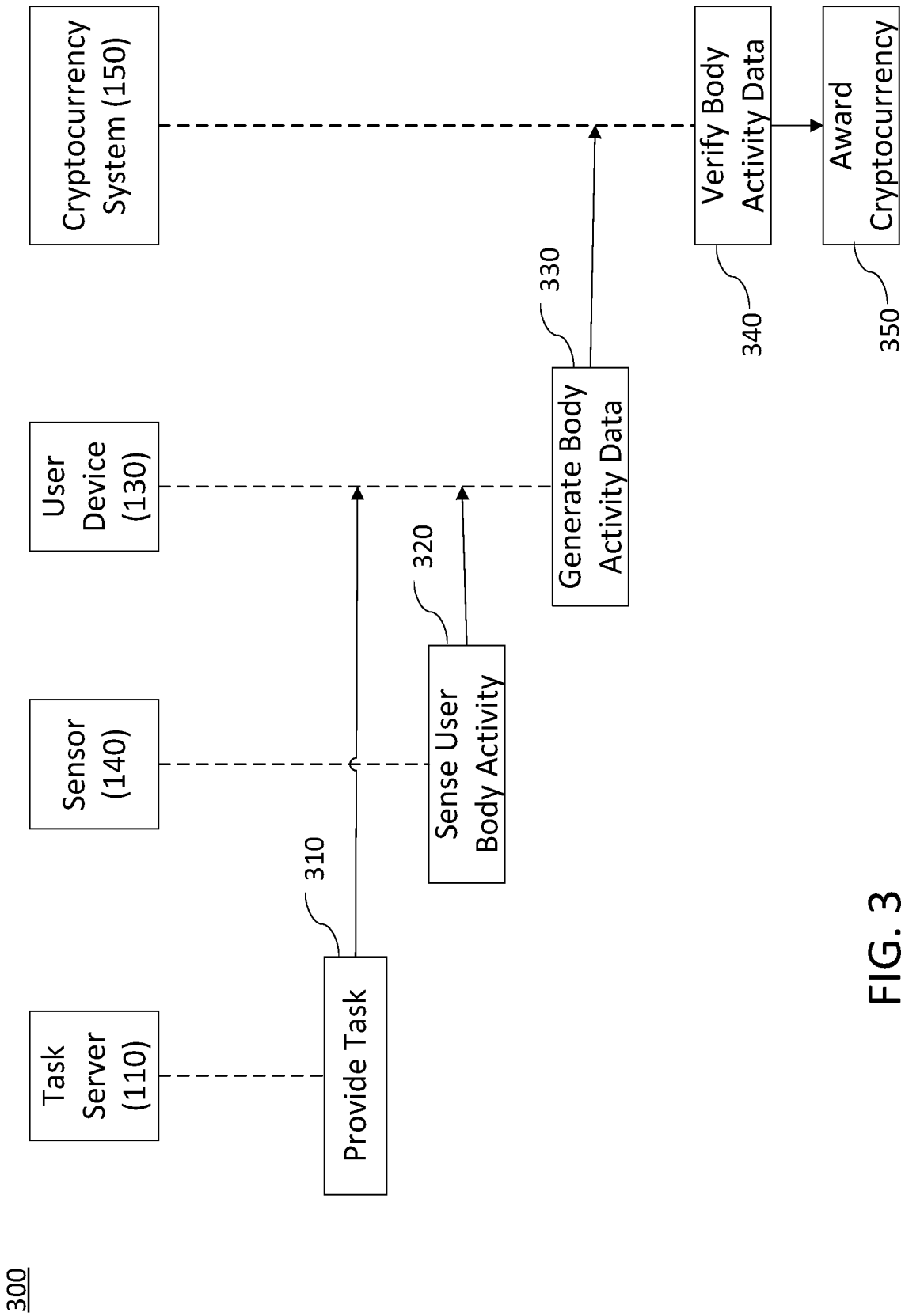

300
Task Server (110)
Sensor (140)
User Device (130)
Cryptocurrency System (150)
Provide Task
310
Sense User Body Activity
320
Generate Body Activity Data
330
Verify Body Activity Data
340
Award Cryptocurrency
350

FIG. 3

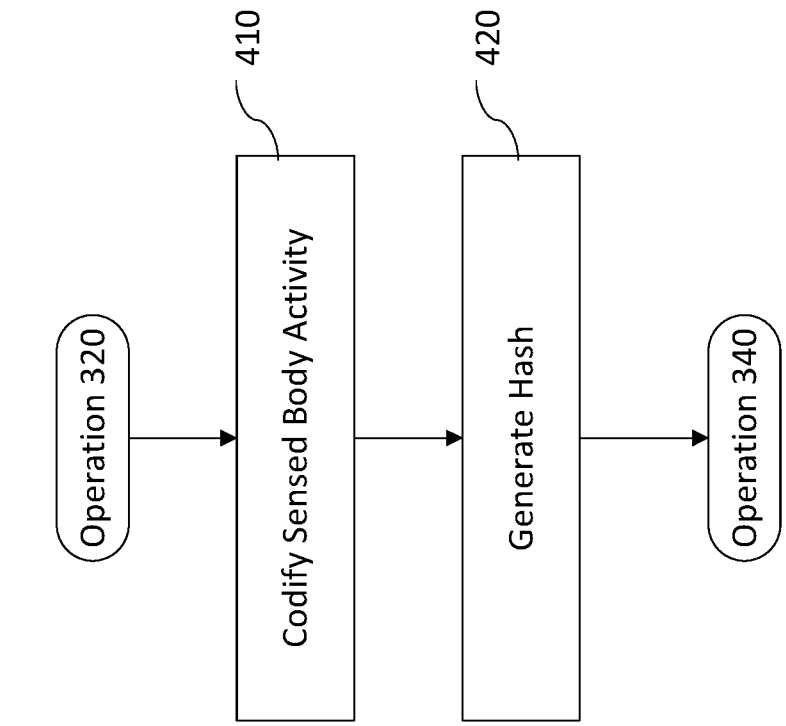

330
Operation 320
410
Codify Sensed Body Activity
420
Generate Hash
Operation 340

FIG. 4

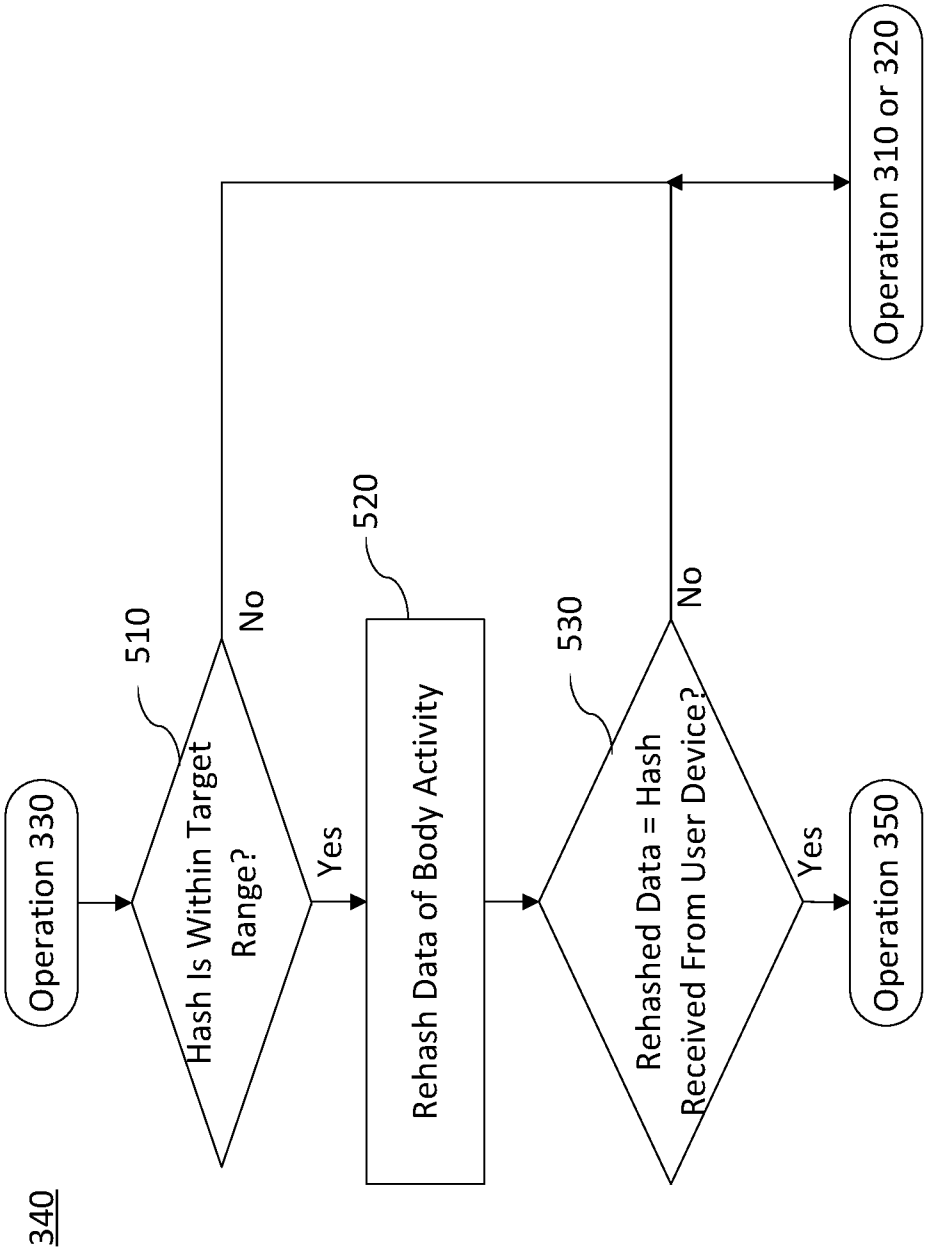

340
Operation 330
Hash Is Within Target Range?
510
No
Yes
Rehash Data of Body Activity
520
Rehashed Data = Hash Received From User Device?
530
No
Yes
Operation 310 or 320
Operation 350

FIG. 5

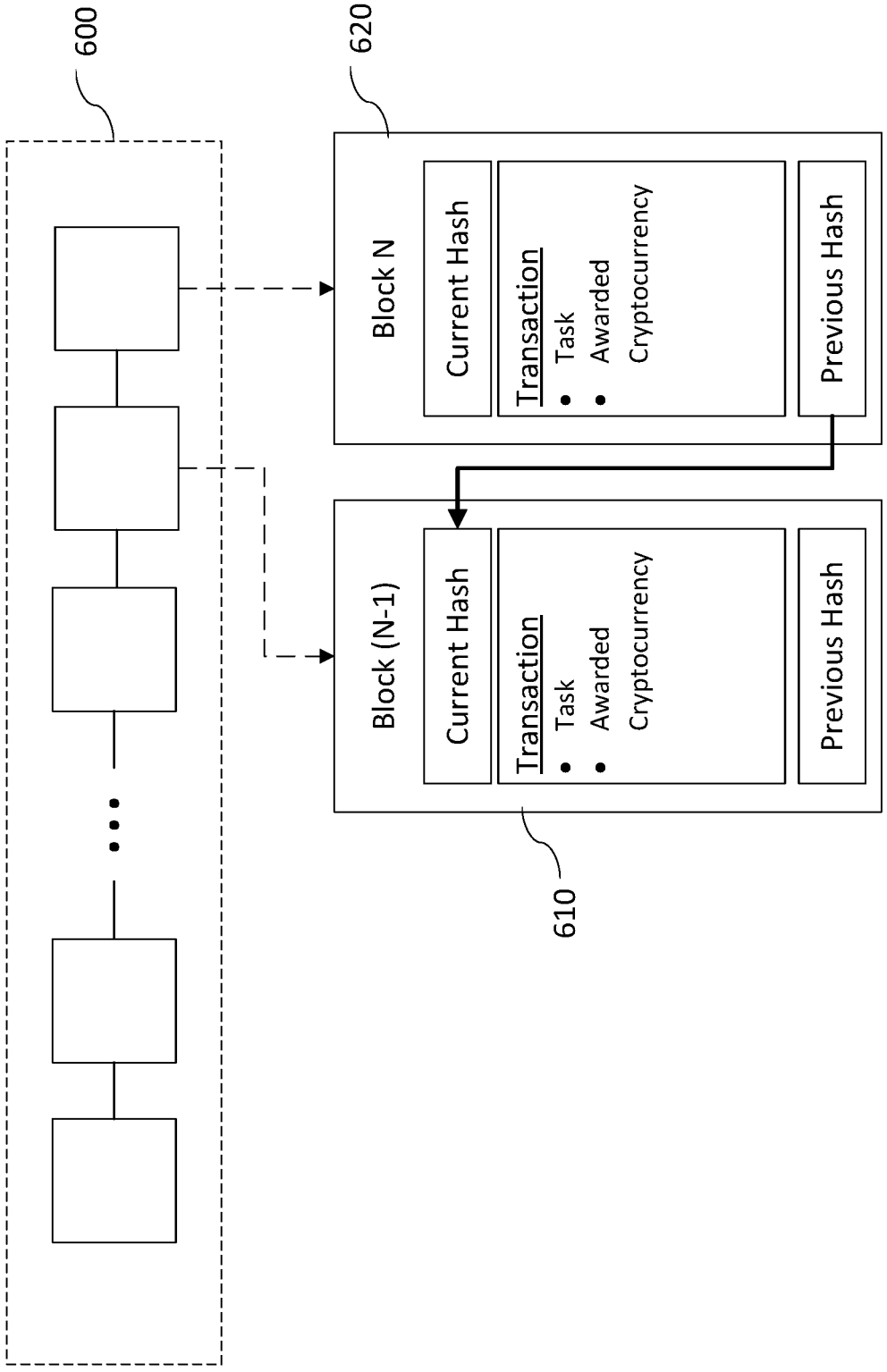

600
620
Block N
Current Hash
Transaction
• Task
• Awarded Cryptocurrency
Previous Hash
Block (N-1)
Current Hash
Transaction
• Task
• Awarded Cryptocurrency
Previous Hash
610

FIG. 6

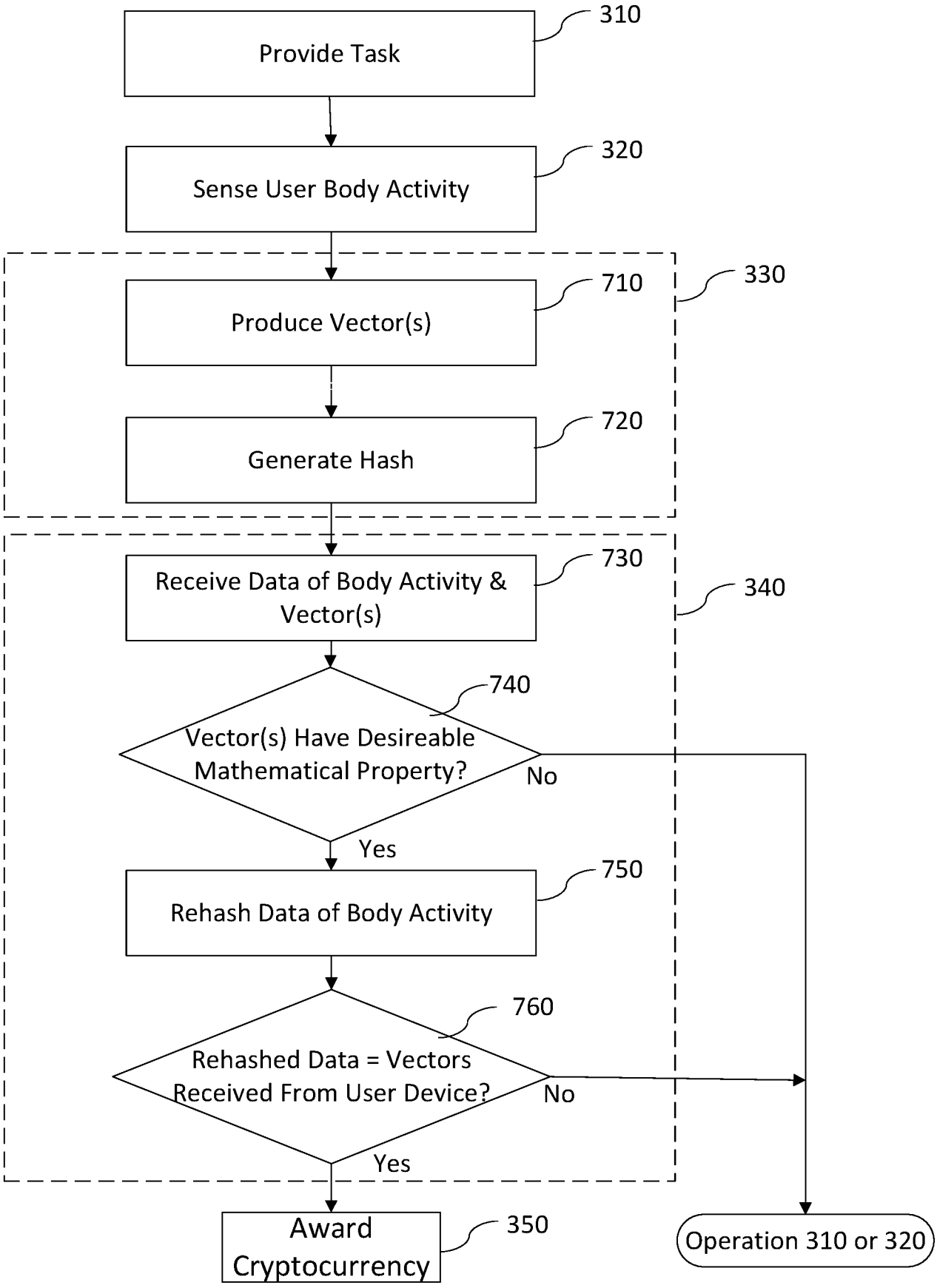

Provide Task
310
Sense User Body Activity
320
330
Produce Vector(s)
710
Generate Hash
720
340
Receive Data of Body Activity & Vector(s)
730
Vector(s) Have Desireable Mathematical Property?
740
No
Yes
Rehash Data of Body Activity
750
Rehashed Data = Vectors Received From User Device?
760
No
Yes
Award Cryptocurrency
350
Operation 310 or 320

FIG. 7

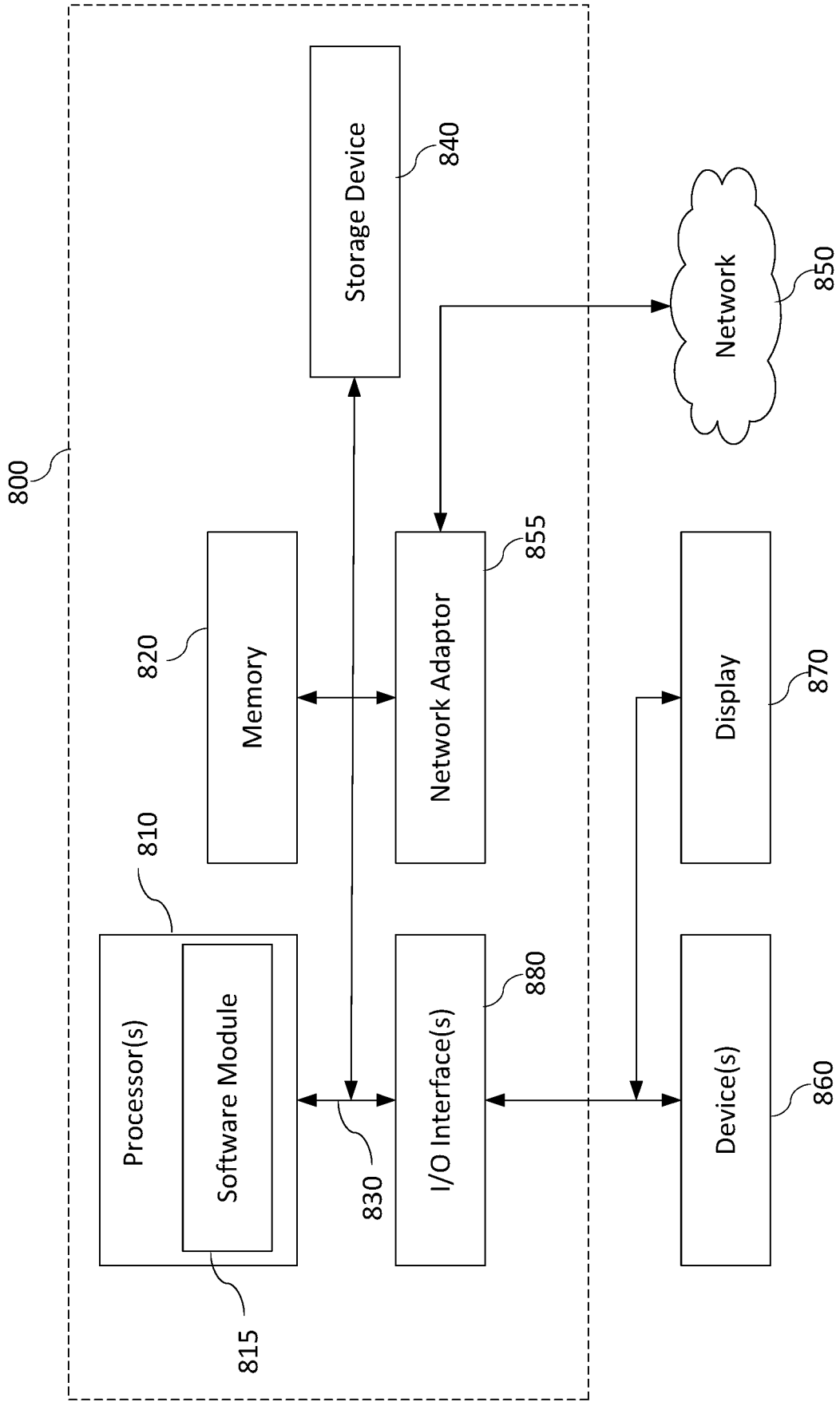

800
Storage Device
840
Network
850
Memory
820
Network Adaptor
855
Display
870
Processor(s)
810
Software Module
815
I/O Interface(s)
880
830
Device(s)
860

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2019/038084

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/06 G06Q20/32 H04L9/32 G06Q30/02 G06N3/08
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q H04L G07G G06N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Neurogress ET AL: "MECHATRONIC SYSTEMS CONTROL VIA NEURAL INTERFACE NEUROGRESS", , 8 February 2018 (2018-02-08), XP055612926, Retrieved from the Internet: URL:https://s3.eu-central-1.amazonaws.com/icostars-whitepapers/d525e659fddaebc1186474abc02142360577982f85787d1086372b1f0668f4c0.pdf [retrieved on 2019-08-14] the whole document ----- -/--	1-15

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 August 2019	27/08/2019

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Veshi, Erzim

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Lisa Barwick: "Researchers help digital currency users get more rewards for exercising", , 14 August 2017 (2017-08-14), XP055613045, Retrieved from the Internet: URL:https://warwick.ac.uk/newsandevents/pressreleases/researchers_help_digital/ [retrieved on 2019-08-14] the whole document	1-15
A	US 2018/247191 A1 (KATZ RANDALL M [US] ET AL) 30 August 2018 (2018-08-30) paragraph [0069] - paragraph [0124]	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2019/038084

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2018247191 A1	30-08-2018	US 2018247191 A1	30-08-2018
		US 2018341861 A1	29-11-2018
		US 2018373983 A1	27-12-2018
		US 2018373984 A1	27-12-2018